Beratung und Support
Technische Plattform
Support-Netz-Portal

paedML® – stabil und zuverlässig vernetzen

Installationsanleitung

Installationsanleitung

Stand 11.06.2015

paedML® Linux

Version: 6.0

paedML® Die Musterlösung für schulische Computernetze

LMZ Landesmedienzentrum Baden-Württemberg

Impressum

Herausgeber

Landesmedienzentrum Baden-Württemberg (LMZ)
Support-Netz
Rotenbergstraße 111

70190 Stuttgart

Autoren

der Zentralen Expertengruppe Netze (ZEN),
Support-Netz, LMZ

Alexander Mittag, Roland Walter, Michael Salm

Endredaktion

Redaktion Support-Netz

Bildnachweis Titelbilder:

Thinkstock

Weitere Informationen

www.support-netz.de
www.lmz-bw.de

Änderungen und Irrtümer vorbehalten.

Veröffentlicht: 2015

Die Nutzung dieses Handbuches ist ausschließlich für eigene Zwecke zulässig. Die Nutzung sowie die Weitergabe dieses Handbuches zu kommerziellen Zwecken wie z.B. Schulungen ist nur nach ausdrücklicher Einwilligung durch das LMZ erlaubt.

© Landesmedienzentrum Baden-Württemberg

Inhaltsverzeichnis

1. Grundlagen der paedML Linux 6.0 10
1.1 Server, Firewall und AdminVM 10
1.2 Virtualisierung 10
1.3 Management-PC 11
1.4 Netzübersicht 12
1.5 Schematische Übersicht über die paedML Linux 6.0 12
2. Vorbereitung des Virtualisierungs-Hosts 14
2.1 Download des Installationsmediums 14
2.2 Beschaffung eines schulspezifischen Lizenzschlüssels 14
2.3 Download von „VMware vSphere-Client“ 14
2.4 Installation des Hypervisors auf dem Virtualisierungs-Host 15
2.5 Anschluss des Virtualisierungs-Hosts an die Netzwerkinfrastruktur der Schule 20
2.6 Grundlegende Konfiguration Virtualisierungs-Host 21
2.6.1 Verbinden der physischen NIC mit dem Netz „INTERNET“ 22
2.6.2 Auswahl der Netzwerkkarte für das „Management Network“ 22
2.6.3 Setzen der IP-Adresse im „Management-Network“ 24
2.6.4 Deaktivieren von IPv6 24
2.6.5 Konfigurieren von DNS und Hostname 25
2.6.6 Durchführen der Änderungen und Neustart des Virtualisierungs-Hosts 26
2.6.7 Test der DNS-Namensauflösung 27
2.6.8 Test der Erreichbarkeit des Virtualisierungs-Hosts 28
2.7 Installation des vSphere-Clients 29
2.7.1 Downloadmöglichkeit des vSphere-Clients 29
2.7.2 Installation des vSphere-Clients 30
2.7.3 Zugriff vom vSphere-Client auf den Hypervisor 30
2.8 Eingabe des Lizenzschlüssels 33
2.9 Zeitsynchronisation des Hypervisors 35
3. Konfiguration der virtuellen Netzwerke 40
3.1.1 Definition virtuelles Netzwerk „INTERNET“ 40
3.1.2 Definition virtuelles Netzwerk „PAEDAGOGIK“ 42
3.1.3 Definition virtuelles Netzwerk „GAESTE“ 45
3.1.4 Überprüfen der virtuellen Netze 48
4. Import der virtuellen Maschinen 49
4.1 Anlegen von Ressourcenpools 49
4.2 Import der VM „Firewall“ 51
4.3 Import der VM „Server“ 59
4.4 Import der VM „opsi-Server“ 67
4.5 Import der VM „AdminVM“ 75
4.6 Überprüfen des Imports 84

5. Basiskonfiguration der virtuellen Maschinen 87

5.1 Basiskonfiguration der VM „Firewall“ 87
5.1.1 IP-Konfiguration der externen Netzwerkkarte 88
5.2 Basiskonfiguration der VM „Server“ 93
5.2.1 Durchführen der Systemindividualisierung 93
5.2.2 Optional: Ändern des Passwortes von „domadmin“ 96
5.2.3 Aktualisieren des Basissystems der VM „Server“ 97
5.3 Basiskonfiguration der VM „opsi-Server“ 98
5.3.1 Aktualisieren des Basissystems der VM „opsi-Server“ 98
5.3.2 Aktualisieren der opsi-Produkte 99
5.4 Updaten der Firewall 100
5.5 OpenVM-Tools aktualisieren 102

6. Ausrollen der VM „AdminVM“ 104

6.1 Import der VM aus OVF-Vorlage 104
6.2 Bereitstellen des Windows-Installationsmediums unter opsi 104
6.3 Aufnahme der AdminVM über die Schulkonsole 105
6.4 Einstellungen in opsi 110
6.4.1 Anmelden im opsi-configed 110
6.4.2 Konfiguration der AdminVM 113
6.5 Ausrollen des Betriebssystems 117
6.6 Installation der VMware-Tools in der AdminVM 117
6.7 Ändern der Gruppenzugehörigkeit der AdminVM 124
6.8 Ändern der Proxy-Einstellungen auf der AdminVM 126
6.9 RDP-Zugriff auf die AdminVM 128
6.9.1 Einrichten der AdminVM für den RDP-Zugriff 128
6.9.2 Test des Zugriffs per RDP auf die AdminVM 133

7. Automatischer Start der virtuellen Maschinen 136

7.1 Einrichtung des automatischen Starts 136

8. Rahmenbedingungen für die Backuplösung 138

8.1 Grundsätzliches zum Betrieb einer NAS 138
8.2 Anbindung der NAS ins Netz 138
8.3 NFS-Share einrichten 139

9. Starten und Stoppen von virtuellen Maschinen 140

9.1 Starten von virtuellen Maschinen 140
9.2 Startreihenfolge 140
9.3 Herunterfahren und Neustart virtueller Maschinen 141
9.3.1 Herunterfahren über die Konsole des Betriebssystems 141
9.3.2 Herunterfahren / Neustart durch vSphere-Client 143
9.4 Hartes Ausschalten/ Harter Neustart 145

10. Snapshots der virtuellen Maschinen 147

10.1 Grundsätzliche Informationen zu Snapshots 147
10.2 Erstellen von Snapshots von „Server“ und „opsi-Server“ 147

10.3 Wiederherstellen eines Snapshots 149
10.4 Verwalten von Snapshots 152
10.5 Snapshots der Firewall 152
10.6 Snapshots weiterer virtueller Maschinen 153

11. Erweiterungsmöglichkeiten der *paedML Linux* 154

11.1 Integration weiterer Server 154
11.2 Vergrößern der Festplatten der VM „Server“ 155
11.2.1 Hinzufügen einer Festplatte zu einer virtuellen Maschine 155
11.2.2 Vorbereiten der neuen Festplatte 161

Einführung

Vielen Dank, dass Sie sich für die *paedML Linux* entschieden haben. Die *paedML Linux 6.0* ist eine Neuentwicklung, die im Vergleich zu ihren Vorgängerversionen mit einem komplett neuen Server- und Clientmanagement ausgestattet wurde. *Univention Corporate Server („UCS*“ mit der Applikation *UCS@school*) bilden nun die technologische Plattform für die Schul-IT-Komplettlösung. Damit ist dje *paedML* hervorragend geeignet, um IT-Infrastrukturen im Schulumfeld bereitzustellen und zu verwalten. Für Lehrkräfte wurde die Anwenderoberfläche neu gestaltet und mit einer intuitiven „*Schulkonsole*“ ausgestattet. Hinzugekommen sind neue Steuerungsfunktionen, die den Lehrkräften noch mehr Sicherheit beim Unterrichten geben (zum Beispiel „Schülercomputer steuern“, „Klassenarbeiten schreiben“, „Internet verwalten“ oder „Drucker moderieren“). Die neue Version ermöglicht deutlich mehr Mobilität beim Lernen, denn Schülerinnen und Schüler können auch mit ihren privaten Geräten im „*Gäste-Netz*“ der Schule arbeiten („*Bring Your Own Device*“). Schuleigene Geräte sind im pädagogischen Schulnetz integriert.

Neben den Verbesserungen für den aktiven Unterrichtablauf bringt die *paedML Linux 6.0* auch für Netzwerkbetreuer deutliche Arbeitserleichterungen mit sich: Viele Installationsroutinen wurden automatisiert. Das beginnt mit einem vereinfachten und weniger fehleranfälligen Installationsverfahren (der *paedML* -Server) mittels Virtualisierung. Außerdem erfolgen Betriebssysteminstallation und Softwareverteilung weitgehend automatisch mit einer Open Source Software (*Open Server Integration – opsi)*. Die Restaurierung wurde ebenso deutlich verbessert, sodass jetzt einzelne oder die gesamten Schüler-Computer in einem Klassenraum innerhalb kürzester Zeit wiederhergestellt werden können.

Mit der *paedML Linux 6.0* haben Sie sich für eine moderne IT-Lösung entschieden, die mit einem professionellen technischen Unterbau ausgestattet ist. Verlässlichkeit und Stabilität kennzeichnen die neue Version, denn Hardwareunterstützung und die Handhabung wurden deutlich verbessert. Technologisch gesehen ist die *paedML Linux 6.0* stärker modular aufgebaut, wodurch die weitere Produktentwicklung in Zukunft flexibler gestaltet werden kann. Wir sind an der Rückmeldung unserer Kunden interessiert und wenn Sie Anregungen oder Wünsche für die Weiterentwicklung der *paedML Linux* haben, bitten wir Sie um Rückmeldung z. B. über unseren User-Helpdesk.

Die Hotline steht Ihnen mit Rat und Tat zur Seite, um Sie in der Administration Ihres schulischen Netzwerks zu unterstützen. Die Erfahrung hat gezeigt, dass es ratsam ist, lieber einmal zu viel, als einmal zu wenig in der Hotline anzurufen. Wenn Sie Fragen zu Ihrer *paedML Linux* haben, dann kontaktieren Sie bitte Ihre Supportmitarbeiter.

Linux Hotline
0711 – 25 35 83 88
linux-hotline@lmz-bw.de
Geschäftszeiten:
Montag – Donnerstag 8.00 – 16.00 Uhr
Freitag 8.00 – 14.30 Uhr

Es gibt drei Handbücher für die *paedML Linux*:

- Die hier vorliegende „**Installationsanleitung**“, welche die Einrichtung von VMware, das Aufsetzen der *paedML Linux* Infrastruktur und den technischen Aufbau des *paedML Linux*-Netzwerks behandelt. Diese Anleitung richtet sich an *Dienstleister*, die die *paedML Linux* einrichten.Das „**Administrationshandbuch**“ richtet sich an den *Netzwerkberater* als Systembetreuer der Schule und an den *Dienstleister*. In diesem Handbuch werden administrative Aufgaben beschrieben, die im Schulalltag getätigt werden können. Darüber hinaus werden dort auch administrative Aufgaben bei der Einrichtung des Schulnetzes beschrieben, die primäre Aufgabe des Dienstleisters ist, der das Schulnetz einrichtet.
- Das „**Handbuch für Lehrkräfte**“, welches die pädagogischen Funktionen Ihrer *paedML Linux* näher beschreibt, erläutert relevante Module für den Unterricht..

Neben diesen drei Handbüchern gibt es weitere Dokumente, die Sie bei der Planung und dem Aufbau eines *paedML Linux* Netzwerkes unterstützen.

- Der „**Konzeptionsleitfaden**“ ist eine kurzeinführung in die paedML Linux. Dieses Dokument enthält Hinweise zur Planung der Installation des schulischen Netzwerkes.
- Hinweise für die Ausschreibung des schulischen Netzes und bei der Übergabe des Netzwerks von Ihrem Dienstleister an die Schule finden Sie in unserem „**Ausschreibungsleitfaden**“.
- In einem weiteren Dokument haben wir die „**Hardwareanforderungen**“ der paedML Linux 6.0 zusammengefasst.

Um Doppellungen zu vermeiden haben wir unsere Handreichungen dergestalt gegliedert, dass wir an gegebener Stelle auf die anderen Handbücher verweisen.

Alle hier genannten Handreichungen zur paedML Linux finden Sie unter http://www.lmz-bw.de/technische-unterstuetzung/kundenportal/linux/dokumentationen.html .

Überprüfen Sie diese Seite bitte regelmäßig nach Aktualisierungen!

Typografische Konventionen

Zur besseren Lesbarkeit werden bestimmte Elemente typografisch vom Rest des Textes abgehoben.

- Hervorhebungen in diesem Dokument sind *kursiv*.
- Besondere Hervorhebungen sind **fett** ausgezeichnet.
- Ausgaben oder Abfragen von Programmen sind *„kursiv und erhalten Anführungszeichen“*. Ebenso werden Menüs oder Knöpfe, in Programmen und Bedienoberflächen mit Anführungszeichen hervorgehoben.
- Vom Benutzer auszuführende Tastatureingaben an der Linux-Konsole oder an der *Windows* Eingabeaufforderung (zum Beispiel Systembefehle) sowie Auszüge aus Systemdateien, werden durch die `Darstellung in Courier New` vom Rest des Textes abgesetzt. Das gleiche gilt für Zugangsdaten wie Benutzernamen oder Passwörter.
- Tastenbeschriftungen werden durch Rahmen hervorgehoben.
- Verschachtelte Menüstrukturen werden durch einen senkrechten Strich (|) als Trennzeichen (in der Linux Welt auch „*Pipe*“[1] genannt) voneinander getrennt. So finden Sie zum Beispiel den Zugriff für das Helpdesk-Modul unter „*Schulkonsole: Unterricht* | *Helpdesk kontaktieren*“.

Unter einigen Kapitelüberschriften finden Sie einen Hinweis, wie Sie den in dem Kapitel beschriebenen Baustein der *paedML Linux* aufrufen können. In der Regel werden konfigurative Änderungen, die in diesem Handbuch beschrieben sind, vom Netzwerkberater ausgeführt. Manche Menüs sind jedoch nur für den Administrator zugänglich. Diese Ausnahmen werden durch Nennung des vom Benutzer „*netzwerkberater*“ abweichenden Benutzernamens gekennzeichnet.

Beispiele:

Aufruf über Schulkonsole (Administrator): Unterricht | Computerraum
Adresse: https://server.paedml-linux.lokal/nagios

Der Aufruf aller internen Webseiten der *paedML Linux* muss über den FQDN (voll qualifizierten Domain-Namen) der jeweiligen Seite geschehen.

Es genügt also nicht bspw. https://server/horde einzugeben, um die Startseite des Webmailers aufzurufen.

Nutzen Sie stattdessen https://server.paedml-linux.lokal/horde .

Hinweise und Tipps werden durch besondere Symbole grafisch vom Text abgehoben:

[1] http://de.wikipedia.org/wiki/Pipe_%28Informatik%29

Durch Hinweis-Felder, werden Sie auf Sachverhalte hingewiesen, die Sie beachten sollten, um bestimmte Probleme zu vermeiden, die den Betrieb der *paedML Linux* beeinträchtigen könnten.

Das Tipp-Feld gibt Hinweise, die nicht zwingend notwendig aber hilfreich sind.

Dieses Feld kennzeichnet Inhalte, die nicht von der Hotline unterstützt werden.

Es handelt sich einerseits um Funktionen und Programme, die nicht Bestandteil der Entwicklung der paedML Linux sind. Diese Programme sind in der Regel zu komplex und zu umfangreich, um in Ihrer Tiefe durch die Hotline unterstützt werden zu können.

Andererseits bewirken Änderungen in den beschriebenen Funktionen, Abweichungen von Standardeinstellungen der paedML Linux[2].

Aufgrund der besseren Lesbarkeit wird in diesem Handbuch die männliche Form verwendet. Die weibliche Form ist selbstverständlich immer mit eingeschlossen.

[2] In der Entwicklung unserer Produkte setzen wir Standards, die durch die Hotline unterstützt werden (können). Wir bitten Sie um Verständnis, dass es unseren Mitarbeitern nicht möglich ist auf alle Bedürfnisse en Detail einzugehen. Wir können Ihnen bei manchen Anfragen lediglich Hinweise geben, wie Sie Änderungen am System vornehmen oder wo Sie weitere Dokumentationen zu dem Thema finden können.

1. Grundlagen der paedML Linux 6.0

Die *paedML Linux 6.0* ist eine vollständige Neuentwicklung und unterscheidet sich grundlegend von den Vorgängerversionen. So besteht die *paedML Linux 6.0* im Auslieferungszustand aus drei Servern. Zusätzlich wird ein *Windows*-Rechner für die Aktivierung von Windows-Lizenzen, die sogenannte AdminVM benötigt. Diese Geräte werden virtualisiert installiert.

Im Folgenden soll ein Überblick über den Aufbau und die Nomenklatur der *paedML Linux* gegeben werden. Weitergehende Ausführungen finden sich im ersten Kapitel des Administrator-Handbuches.

1.1 Server, Firewall und AdminVM

Die *paedML Linux* basiert in der Standardkonfiguration auf den folgenden vier virtuellen Maschinen mit unterschiedlichen Funktionen:

virtuelle Maschine	Funktionen (auszugsweise)
VM „*Server*“	Benutzerauthentifizierung File-Server (Benutzerverzeichnisse) Administration des Systems (Schulkonsole) Proxy-Server Steuerung des Internetzugriffs
VM „*opsi-Server*“	Client-Management (Ausrollen der Betriebssysteme, Softwareverteilung). Aus Gründen, die dem Unterbau auf *Univention Corporate Server* geschuldet sind, lautet die Bezeichnung an manchen Stellen auch „*backup*“.
VM „*Firewall*“	Die Firewall trennt die internen Netze (pädagogisches Netz, Lehrernetz, Gäste-Netz) und stellt den Internetzugang für diese Netze bereit. Die Firewall bietet eine Reihe von Filtermöglichkeiten.
VM „*AdminVM*“	virtuelle Maschine, die unter *Windows 7* (64 bit) läuft. Sie wird für diverse Hilfsdienste (z.B. Gruppenrichtlinien, *Windows*-Aktivierung) benötigt, die zwingend unter *Windows* laufen müssen. Für diese VM wird eine *Windows 7* (64 bit)-Lizenz benötigt.

Tabelle 1: Die virtuellen Maschinen der paedML Linux

1.2 Virtualisierung

Virtualisierungs-Host
Grundlage der Virtualisierung bildet der physische Server, der sogenannte „*Virtualisierungs-Host*“. Dieser muss über genügend Prozessorleistung, Hauptspeicher und Plattenplatz verfügen. Hinweise zur Ausstattung des Virtualisierungs-Hosts finden Sie in unseren Hardwareanforderungs-Dokument unter http://support-netz.de/technische-unterstuetzung/kundenportal/linux/dokumentationen.html.

Hypervisor
Als *Hypervisor* bezeichnet man die Software, die auf dem Virtualisierungs-Host die eigentliche Virtualisierung vornimmt und eine Umgebung für virtuelle Gastsysteme zur Verfügung stellt. Die

paedML Linux basiert auf *VMware vSphere ESXi*, einem nativen Hypervisor, der ohne ein zusätzliches Wirts-Betriebssystem direkt auf der Hardware des Servers läuft.

Virtuelle Maschinen
In der virtuellen Umgebung des Hypervisors werden mehrere virtuelle Maschinen (VM) betrieben. Diese virtuellen Maschinen laufen auf „virtueller Hardware“ und teilen sich die Ressourcen des Virtualisierungs-Hosts.

Konsolenzugriff auf den Hypervisor
Per angeschlossener Tastatur und Monitor kann auf den Hypervisor nur über eine Textoberfläche zugegriffen werden, die ausschließlich zur Basiskonfiguration des Hypervisors selbst dient. Eine Verwaltung oder ein Zugriff auf die virtuellen Maschinen ist darüber nicht möglich.
Sollte es später bei einer versehentlichen Fehlkonfiguration der Netze über die grafische Schnittstelle (s. nächster Abschnitt) zu einem sog. „Lockout“ kommen, d.h. der Zugriff über die grafische Schnittstelle dadurch auf den Hypervisor abgeschnitten sein, so kann über die Textkonsole der Netzzugriff wieder hergestellt werden.

Grafischer Zugriff auf die virtuellen Maschinen
Die Verwaltung der virtuellen Maschinen und der grafische Zugriff erfolgt über die Software „*VMware vSphere Client*“, die auf einem physischen *Windows*-Rechner außerhalb des Virtualisierungs-Hosts installiert sein muss.

Für den Installationsvorgang der *paedML Linux* kann der *vSphere-Client* auch temporär auf einem beliebigen PC (z.B. auf dem Notebook eines IT-Dienstleisters) installiert werden, der per Netzwerk mit dem Virtualisierungs-Host verbunden ist.

Im laufenden Betrieb ist es ebenfalls notwendig, per *vSphere-Client* auf die virtuellen Maschinen zuzugreifen. Hierzu könnte der *vSphere-Client* auf einem beliebigen PC oder Notebook installiert sein. Dieses Gerät muss über das Netzwerk mit dem Virtualisierungs-Host verbunden sein.

1.3 Management-PC

In der vorliegenden Installationsanleitung wird unter dem Begriff *Management-PC* ein physischer PC verstanden, auf dem ein *vSphere-Client* installiert ist. Dieser Rechner ist über das Netzwerk mit dem Virtualisierungs-Host verbunden. Bei der Einrichtung des schulischen Netzes kann ein Rechner des Dienstleisters diese Aufgabe übernehmen.

Vorgehen nach der Installation
Wenn die Installation der *paedML Linux* abgeschlossen ist, wird der *Management-PC* nur noch sporadisch benötigt. Über den *vSphere Client* werden virtuelle Maschinen und/oder der Hypervisor gestartet oder Heruntergefahren. Konfigurative Änderungen an der Virtualisierung werden ebenfalls über den *vSphere Client* durchgeführt.

Obwohl aus „Kostengründen“ auch ein Client-PC temporär als *Management-PC* zweckentfremdet werden könnte, empfehlen wir, für Administrationsaufgaben der *paedML Linux* einen dedizierten *Windows*-PC als *Management-PC* zu verwenden.

Der Vorteil beim Einsatz eines dedizierten Management-PCs im Netzsegment „*Internet*“(vgl. folgender Abschnitt) ist, dass Dienstleister oder die Hotline immer auf das System zugreifen können. Dies gilt

auch, wenn der Virtualisierungs-Server Probleme, da der Zugriff direkt nach dem Router erfolgt. Wenn das Gerät nicht in Benutzung ist, kann es ausgeschaltet werden.

Bei „Management-PC“ und „AdminVM“ handelt es sich um völlig verschiedene Maschinen, die nicht verwechselt werden sollten.

Als Betriebssystem für den Management-PC wird *Windows* 7 (64 Bit) empfohlen.

1.4 Netzübersicht

Innerhalb der *paedML Linux* sind drei Netze definiert:

- „*PAEDAGOGIK*“: Hier befinden sich die Client-Rechner und die Server der *paedML Linux.*
- „*GAESTE*“: Das Gäste-Netz ist für den sicheren Betrieb von nicht zum Schul-Netz gehörigen Rechnern wie Notebooks von Schülern oder Lehrern (Stichwort: „*Bring Your Own Device*“) vorgesehen. Sollen keine schulfremden Geräte an das Schulnetz angeschlossen werden, so kann auf das Gäste-Netz verzichtet werden.
- „*INTERNET*“: Netz für die Internetanbindung und den Management-PC, über den auf den Hypervisor zugegriffen werden kann. In der Nomenklatur des Hypervisors ist dies das sogenannte „*Management-Netz*“.

Die drei Netze können sowohl mit drei physikalisch getrennten Switches, als auch per VLAN über einen management-fähigen Switch betrieben werden. Dies ist von der vorhandenen Netzinfrastruktur der Schule abhängig.

Jedes Netz existiert sowohl außerhalb des Virtualisierungs-Hosts als auch innerhalb der virtualisierten Umgebung, dort existiert für jedes Netz ein „virtueller Switch“ (in der VMware-Nomenklatur „*vSwitch*“).

Innerhalb der virtualisierten Umgebung werden die virtualisierten Netzwerkkarten der VMs „per Mausklick“ mit einem *vSwitch* verbunden und so an das Netz angebunden.

Die physischen Netzwerkkarten des Virtualisierungs-Hosts verbinden den physischen mit dem virtualisierten Teil eines jeden Netzes. Aus Sicht der Netzwerkgeräte (Client-PCs und auch virtualisierte Server) geschieht dies jedoch völlig transparent.

Die Einrichtung und Wartung einer funktionierenden Netzwerk-Infrastruktur ist Aufgabe des Dienstleisters.

Die Mitarbeiter der Hotline können hierbei nur unterstützend wirken.

1.5 Schematische Übersicht über die paedML Linux 6.0

Die folgende Grafik gibt einen Überblick über den Aufbau der *paedML Linux*:

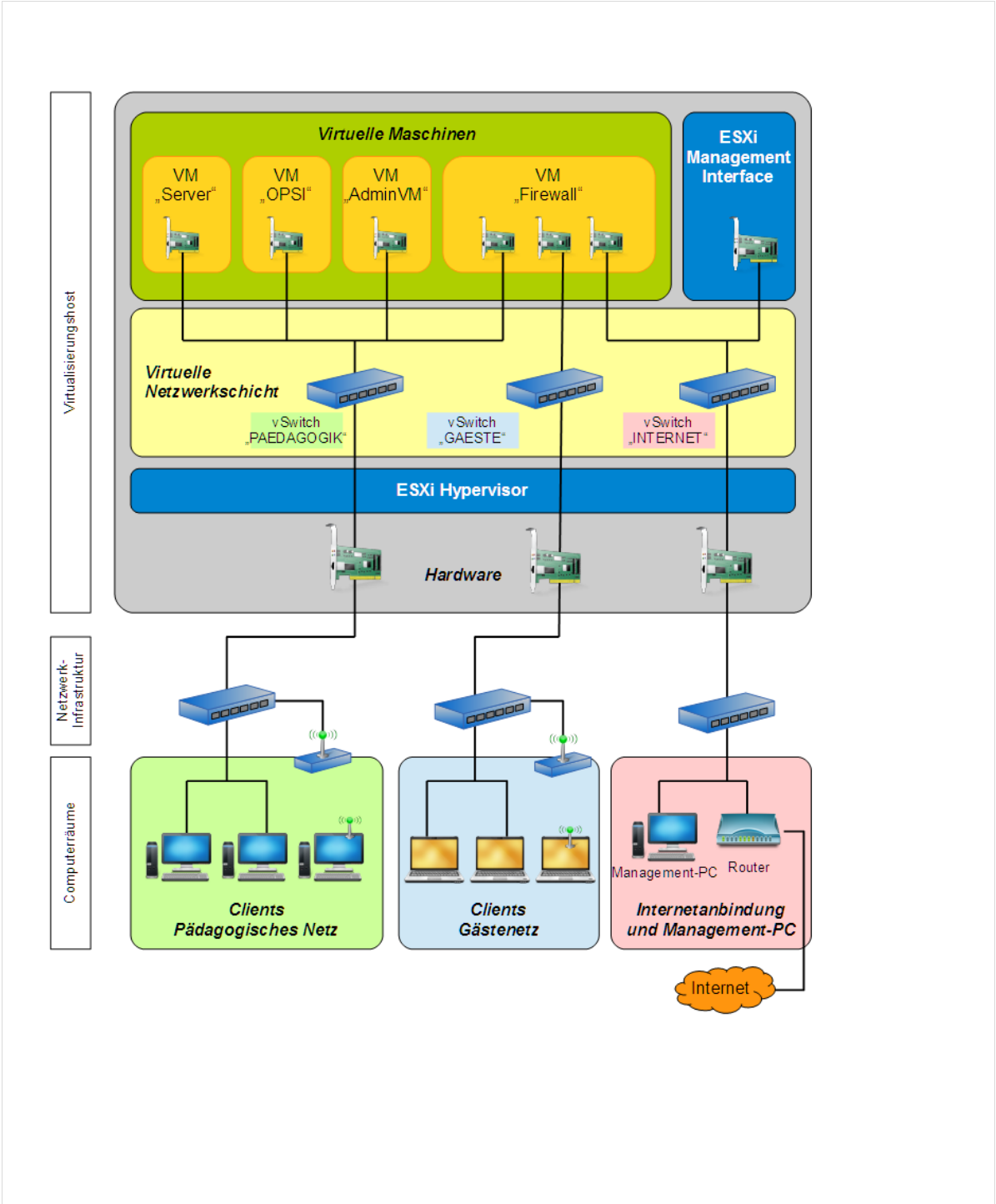


Abb. 1: Schematischer Aufbau der paedML Linux.

2. Vorbereitung des Virtualisierungs-Hosts

Auf dem Virtualisierungs-Host muss zunächst der Hypervisor (Virtualisierungs-Software) installiert werden. In der *paedML Linux* kommt das Produkt „*VMware vSphere Hypervisor (ESXi)*“ in der Version 5.5 zum Einsatz.

In den folgenden Schritten werden Download, Installation und Basiskonfiguration des Hypervisors beschrieben.

2.1 Download des Installationsmediums

Den freien Hypervisor „*VMware vSphere Hypervisor (ESXi)“* können Sie sich auf der Website des Herstellers unter http://www.vmware.com/products/vsphere-hypervisor/ herunterladen. Hierzu ist lediglich eine Registrierung per Emailadresse („*Create an Account*“, bzw. „*Einrichtung Benutzerkonto*“) auf der vorgenannten Website erforderlich. Empfohlen wird die Versionsnummer 5.5, Update 2.

Brennen Sie abschließend das zuvor heruntergeladene ISO-Image des Hypervisors auf CD. Sie benötigen diese im Rahmen des folgenden Installationsprozesses.

2.2 Beschaffung eines schulspezifischen Lizenzschlüssels

Der *vSphere Hypervisor* befindet sich direkt nach der Installation in einem 60 Tage andauernden Testmodus, in welchem er auch im Hinblick auf die teuerste Kaufvariante des vorgenannten Hypervisors zunächst funktional uneingeschränkt ist.

Da für den schulischen Betrieb der Funktionsumfang des kostenlosen Hypervisors meist ausreichend ist, wird empfohlen, die schulische Hypervisor-Installation vor Ort umgehend auf eine zeitlich unbefristete Nutzungsdauer umzustellen, indem Sie den Lizenzschlüssel eingeben.

Der individuelle Lizenzschlüssel für die Schule lässt sich nach Login auf der Herstellerseite mit dem oben erzeugten Benutzerkonto unter der Rubrik „*License & Download*“ abrufen. Am besten speichern Sie diesen Lizenzschlüssel auf einem externen Datenträger (z.B. USB-Stick) ab, da er später noch für die kostenlose Lizensierung des Virtualisierungs-Hosts benötigt wird.

Für spätere Verwendungszwecke (z.B. Neuinstallation des Hypervisors) ist es ratsam den Lizenzschlüssel aufzubewahren.

2.3 Download von „VMware vSphere-Client“

Für den späteren grafischen Zugriff auf die virtuellen Maschinen benötigen Sie das Produkt „*VMware vSphere Client*“, das Sie nach kostenloser Registrierung ebenfalls von den Seiten von VMware beziehen können:

https://www.vmware.com/go/DE-get-esxi

Laden Sie die vSphere-Client-Installationsdatei herunter und speichern Sie diese auf einem Datenträger.

2.4 Installation des Hypervisors auf dem Virtualisierungs-Host

Die eingesetzte Serverhardware sollte grundsätzlich VMware-zertifiziert sein (vgl. https://www.vmware.com/guides.html) und darüber hinaus dem Hardware-Anforderungspapier zur *paedML Linux 6.0* (vgl. http://support-netz.de/technische-unterstuetzung/kundenportal/linux/dokumentationen.html) entsprechen

Legen Sie nun die gebrannte Installations-CD in das optische Laufwerk des Servers ein und booten Sie diesen von CD-ROM.

Wenn Ihr Server auf Booten vom optischen Laufwerk eingestellt ist, erscheint zunächst das folgende Auswahlmenü:

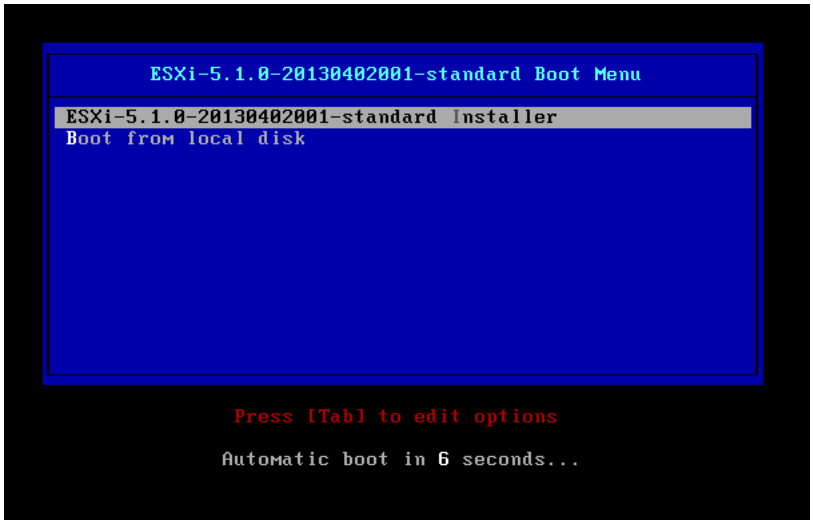


Abb. 2: Auswahl des Bootmediums

Bestätigen Sie den Bootvorgang von der Installer-CD mit Enter. Daraufhin wird das Installer-System von CD gebootet:

Beim Installationsvorgang werden sämtliche Daten auf der Festplatte unwiederbringlich gelöscht!

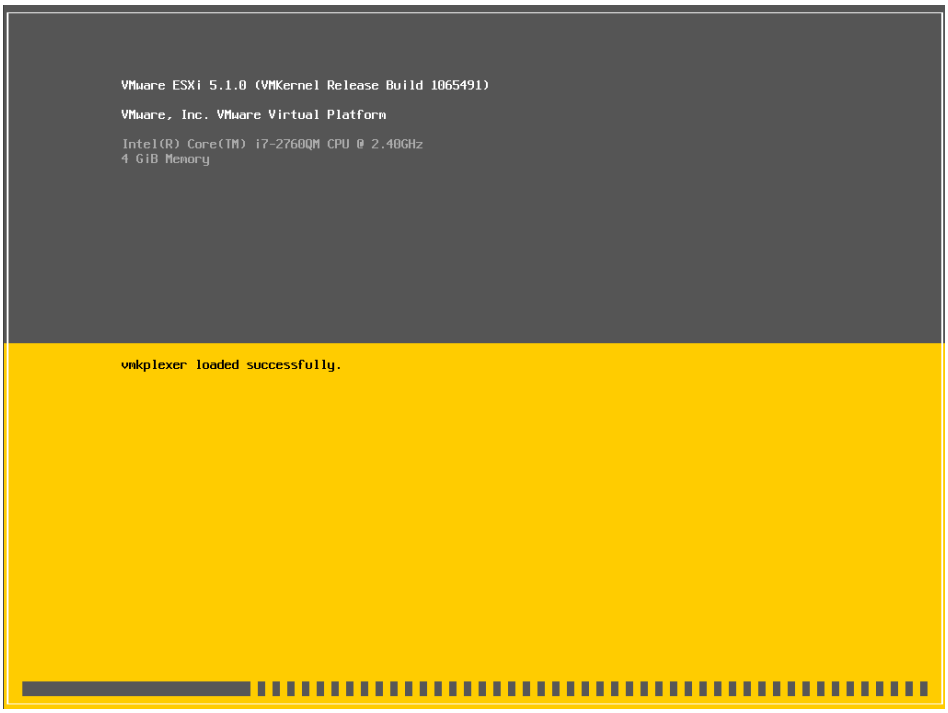

VMware ESXi 5.1.0 (VMKernel Release Build 1065491)
VMware, Inc. VMware Virtual Platform
Intel(R) Core(TM) i7-2760QM CPU @ 2.40GHz
4 GiB Memory
vmkplexer loaded successfully.

Abb. 3: Bootvorgang des Installer-Systems

Nach kurzer Wartezeit wird der Startschirm der Installationsroutine angezeigt. Bestätigen Sie den Start des Installationsvorgangs mit ENTER.

VMware ESXi 5.1.0 Installer
Welcome to the VMware ESXi 5.1.0 Installation
VMware ESXi 5.1.0 installs on most systems but only systems on VMware's Compatibility Guide are supported.
Consult the VMware Compatibility Guide at:
http://www.vmware.com/resources/compatibility
Select the operation to perform.
(Esc) Cancel
(Enter) Continue

Abb. 4: Start der Installation des Hypervisors

Im nächsten Bildschirm werden die Lizenzbedingungen (*End User License Agreement*, kurz *EULA*) angezeigt:

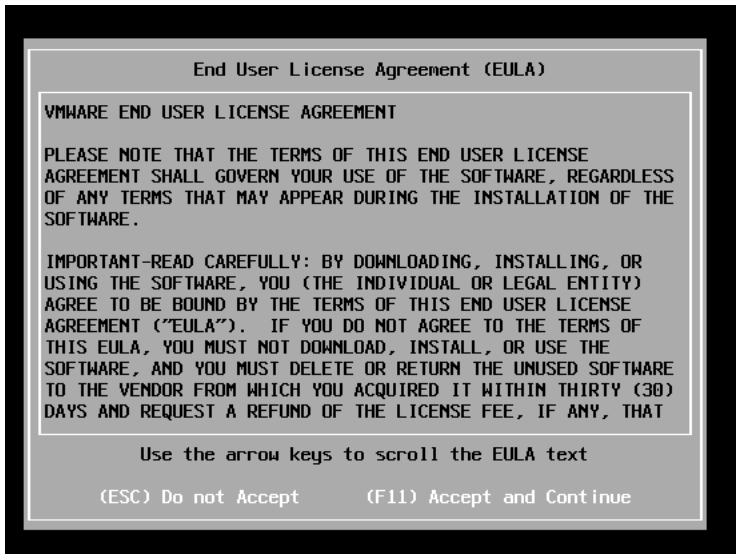

End User License Agreement (EULA)
VMWARE END USER LICENSE AGREEMENT
PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.
IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT
Use the arrow keys to scroll the EULA text
(ESC) Do not Accept
(F11) Accept and Continue

Abb. 5: Bestätigung der Lizenzbedingungen des Hypervisors

Bestätigen Sie mit F11. Der Installer beginnt mit dem Scannen der Hardware.

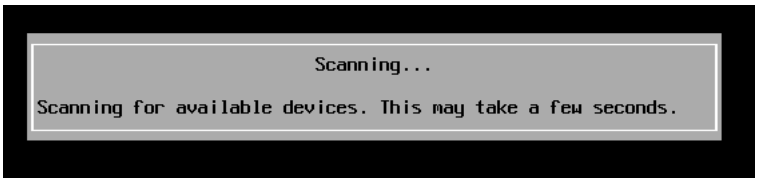


Abb. 6: Scan der Hardware des Virtualisierungs-Hosts

Im nächsten Bildschirm muss die Festplatte für die Installation des Hypervisors ausgewählt werden:

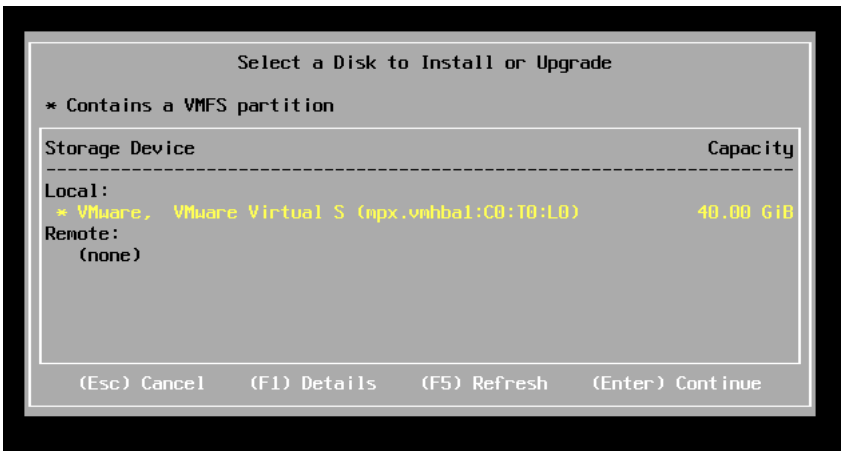


Abb. 7: Auswahl der Festplatte, auf der der Hypervisor installiert wird.

Wählen Sie die Festplatte aus, auf der der Hypervisor installiert werden soll und bestätigen Sie Ihre Wahl mit ENTER.

Im nächsten Bildschirm muss die Tastaturbelegung ausgewählt werden:

Abb. 8: Auswahl der Tastaturbelegung

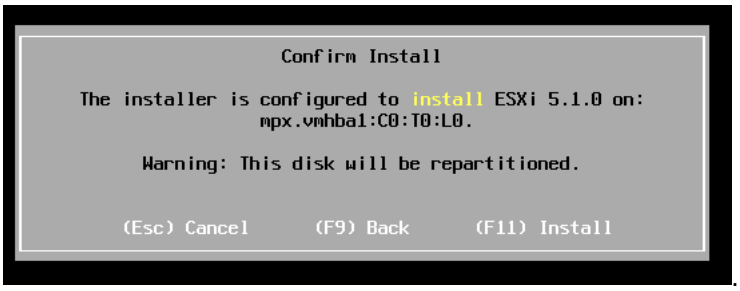
Wählen Sie mit den Pfeiltasten Hoch/Runter die gewünschte Tastaturbelegung aus (typischerweise „*German*“) und bestätigen Sie mit ENTER.

Im nächsten Bildschirm müssen Sie ein *root*-Passwort für die Administration des Hypervisors vergeben:

Abb. 9: Setzen des root-Passworts für den Hypervisor

Geben Sie das *root*-Passwort zweimal ein und bestätigen Sie mit ENTER.

Nach einem weiteren Scan muss die endgültige Installation des Hypervisors nochmals bestätigt werden:



...

Abb. 10: Endgültige Bestätigung der Installation des Hypervisors

Bestätigen Sie die Installation mit ENTER. Daraufhin beginnt der eigentliche Installationsvorgang.

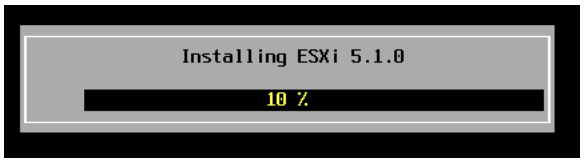


Abb. 11: Installationsvorgang des Hypervisors

Nach erfolgreichem Abschluss des Installationsvorgangs erscheint die folgende Meldung:

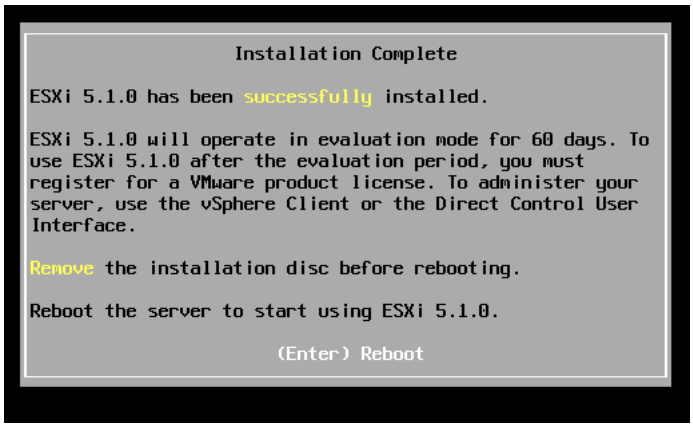

Installation Complete
ESXi 5.1.0 has been successfully installed.
ESXi 5.1.0 will operate in evaluation mode for 60 days. To use ESXi 5.1.0 after the evaluation period, you must register for a VMware product license. To administer your server, use the vSphere Client or the Direct Control User Interface.
Remove the installation disc before rebooting.
Reboot the server to start using ESXi 5.1.0.
(Enter) Reboot

Abb. 12: Der Hypervisor wurde erfolgreich installiert

Bestätigen Sie den Neustart des Systems mit ENTER, das System führt einen Neustart aus:

Abb. 13: Neustart des Systems nach abgeschlossener Installation

Nach dem Neustart des Systems erscheint die Oberfläche des Hypervisors. Damit ist die Basisinstallation des Hypervisors abgeschlossen.

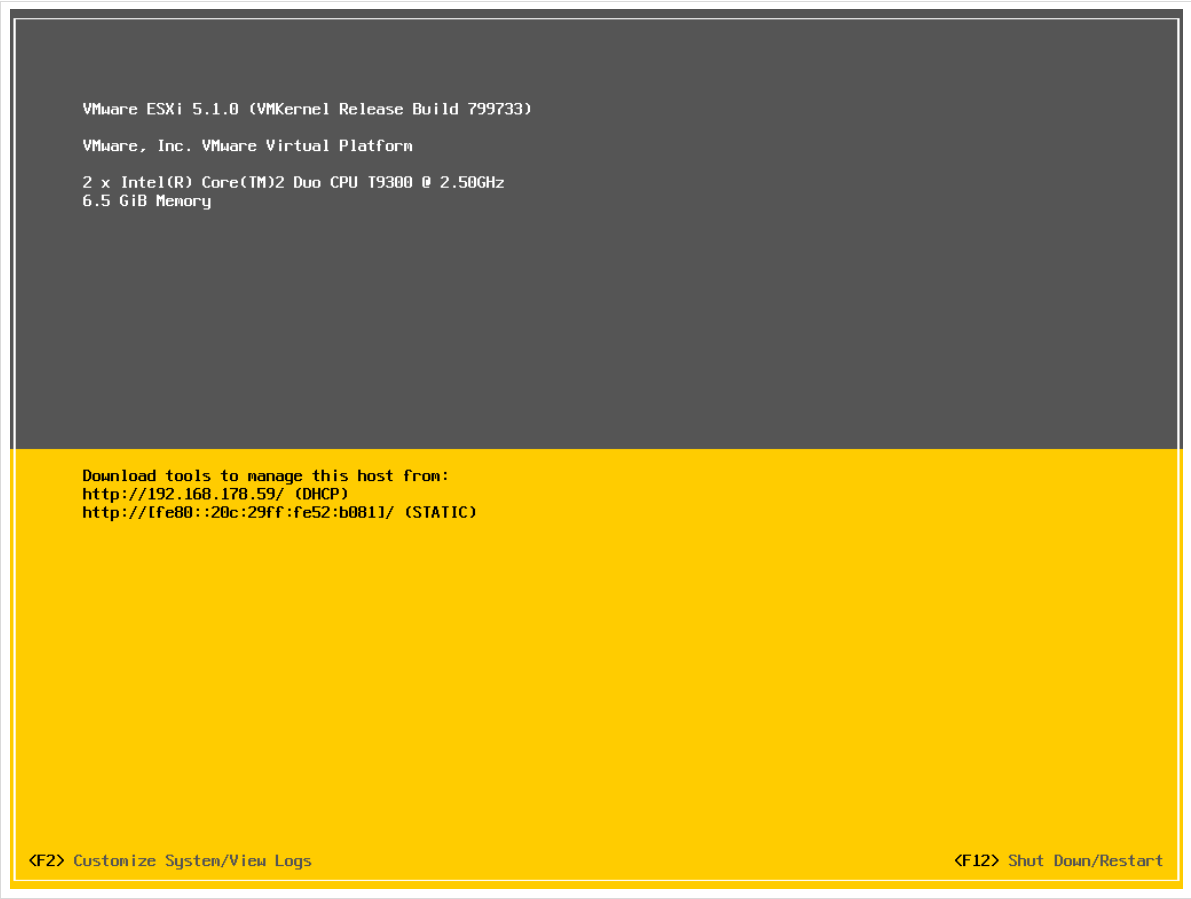

VMware ESXi 5.1.0 (VMKernel Release Build 799733)
VMware, Inc. VMware Virtual Platform
2 x Intel(R) Core(TM)2 Duo CPU T9300 @ 2.50GHz
6.5 GiB Memory
Download tools to manage this host from:
http://192.168.178.59/ (DHCP)
http://[fe80::20c:29ff:fe52:b081]/ (STATIC)
<F2> Customize System/View Logs
<F12> Shut Down/Restart

Abb. 14: Oberfläche des Hypervisors nach dem Neustart

2.5 Anschluss des Virtualisierungs-Hosts an die Netzwerkinfrastruktur der Schule

In der vorliegenden Anleitung wird von den folgenden Prämissen ausgegangen:

Netzbezeichnung	Verwendung
INTERNET	▪ Internetanschluss z.B. über einen DSL-Router wie zum Beispiel *Telekom Speedport*, *FritzBox,…* ▪ Außerdem Zugriff auf den Hypervisor per *vSphere-Client*
PAEDAGOGIK	▪ Netz mit strukturierter Verkabelung und evtl. WLAN für **schuleigene und von der *paedML Linux* verwaltete** Geräte
GAESTE	▪ „*Gäste-Netz*“ mit strukturierter Verkabelung und evtl. WLAN für **schulfremde bzw. nicht von der *paedML Linux* verwaltete** Geräte

Tabelle 2: Die Bezeichnungen der einzelnen Netze

Vor dem Durchführen der im nächsten Abschnitt beschriebenen Arbeiten empfehlen wir, vorerst nur eine der (mindestens) drei im Server vorhandenen Netzwerkkarten per Kabel anzuschließen. Dieses zuerst

eingesteckte Kabel sollte (eventuell über einen Switch) mit einer der LAN-Buchsen Ihres DSL-Routers verbunden sein.

Die schrittweise Vorgehensweise bezüglich der Verkabelung der beiden anderen im Server befindlichen Netzwerkkarten erleichtert die Zuordnung der Karten zu den im Verlauf der Installation noch einzurichtenden virtuellen Netzwerken.

2.6 Grundlegende Konfiguration Virtualisierungs-Host

Nach Abschluss der Basisinstallation und Neustart des Servers finden Sie sich auf der Startseite des Hypervisors wieder. Über die F2-Taste gelangen Sie – nach Eingabe von Benutzername (root) und zugehörigem Passwort – in das Konfigurationsmenü.

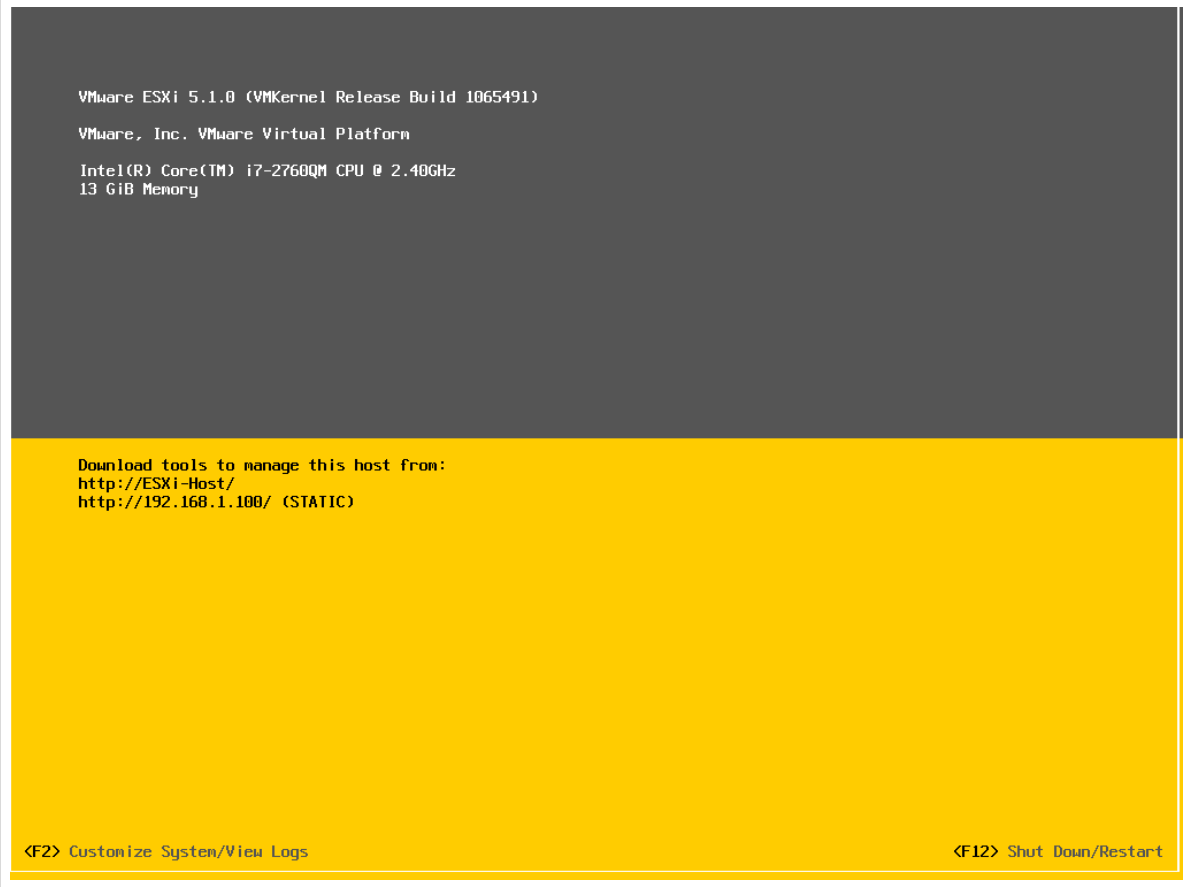

VMware ESXi 5.1.0 (VMKernel Release Build 1065491)
VMware, Inc. VMware Virtual Platform
Intel(R) Core(TM) i7-2760QM CPU @ 2.40GHz
13 GiB Memory
Download tools to manage this host from:
http://ESXi-Host/
http://192.168.1.100/ (STATIC)
<F2> Customize System/View Logs
<F12> Shut Down/Restart

Abb. 15: Hypervisor nach Abschluss der Basisinstallation

Falls im Netz „*INTERNET*“ ein DHCP-Server vorhanden ist (z.B. auf einem DSL-Router), bekommt die externe Netzwerkkarte des Virtualisierungs-Hosts automatisch eine IP-Adresse zugewiesen. Aus Gründen der Wartbarkeit empfehlen wir jedoch, die IP-Adresse des ESX-Servers statisch zu vergeben.

Im Folgenden wird ein Class C Netz verwendet. Der Router wird aus Default-Gateway genutzt und läuft auf der IP-Adresse 192.168.1.1. Der ESXi-Server bekommt die Adresse 192.168.1.100 zugewiesen.

Im Folgenden wird der Virtualisierungs-Host so eingerichtet, dass der Hypervisor per *vSphere-Client* über eine statische IP-Adresse aus dem Netz „*INTERNET*“ erreichbar ist.

Das „Management Network“
In der VMware-Nomenklatur bezeichnet „*Management Network*" das Netzwerk, über das der Hypervisor mittels *vSphere-Client* zu Management-Zwecken erreichbar ist. Bei der Einrichtung der *paedML Linux* wird empfohlen das Management-Netz auf das Netzwerk „*INTERNET*“ zu legen.

2.6.1 Verbinden der physischen NIC mit dem Netz „INTERNET“

Verbinden Sie zunächst nur diejenige Netzwerkkarte (NIC) des Virtualisierungs-Hosts, die für das Netz „*INTERNET*“ vorgesehen ist. Verbinden Sie die Netzwerkkarte per LAN-Kabel mit dem entsprechenden Switch oder direkt mit der LAN-seitigen Buchse des DSL-Routers.

Durch Drücken der F2-Taste und anschließender root-Authentifizierung gelangen Sie in das Menü, in dem Sie die Netzwerkkonfiguration des Virtualisierungs-Hosts anpassen können.

Navigieren Sie per Pfeiltaste auf die Option „*Configure Management Network*“ und bestätigen Sie mit Enter.

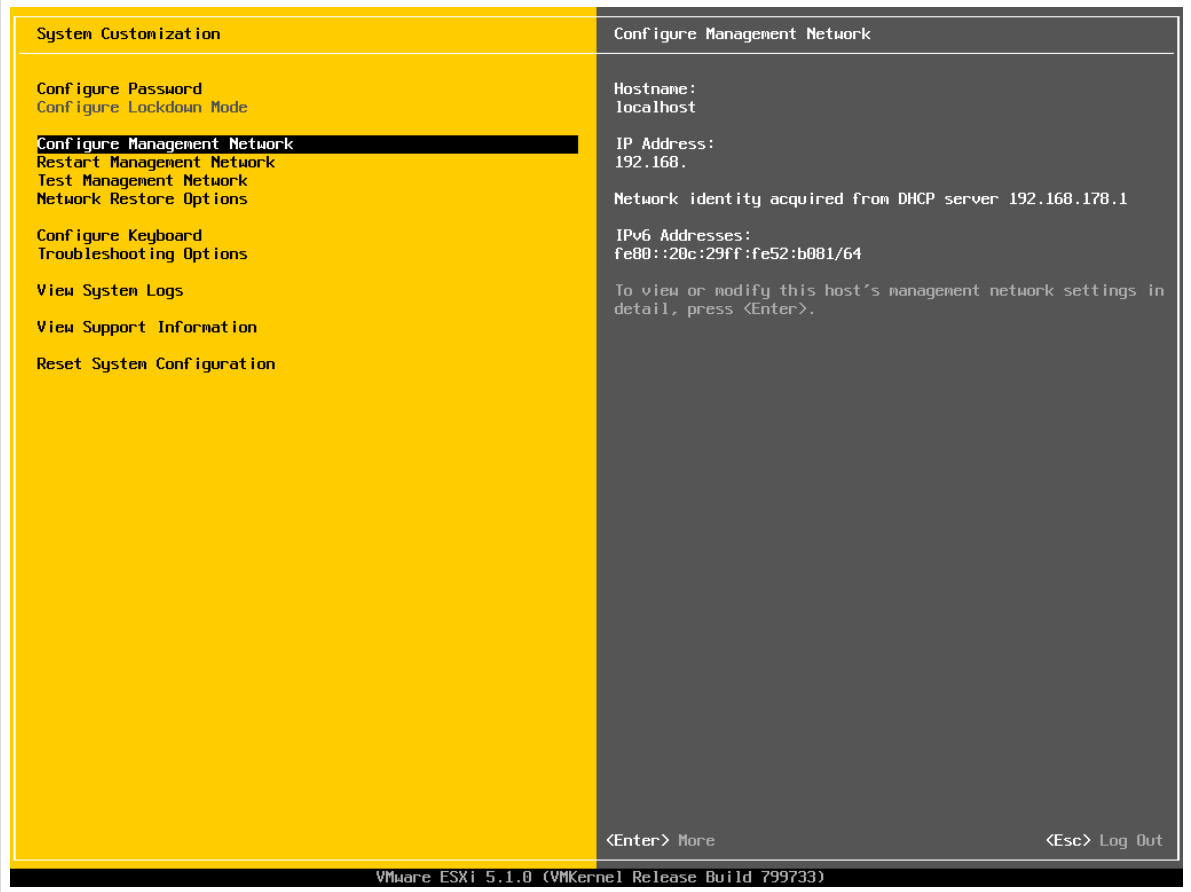


Abb. 16: Hauptmenü zur Konfiguration des Hypervisors

2.6.2 Auswahl der Netzwerkkarte für das „Management Network“

Wählen Sie im nächsten Menü per Pfeiltasten die Option „*Network Adapters*“ aus und bestätigen Sie mit Enter:

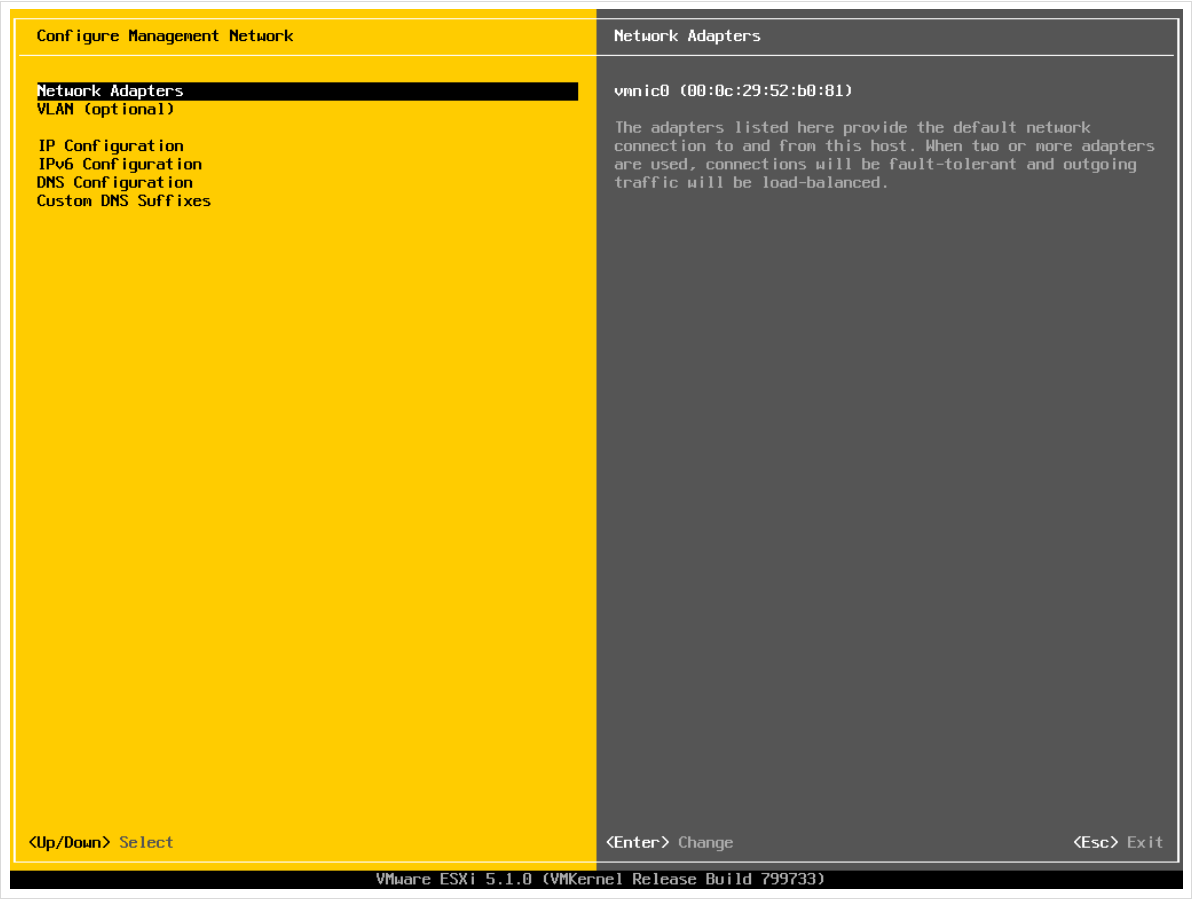

Configure Management Network
Network Adapters
VLAN (optional)
IP Configuration
IPv6 Configuration
DNS Configuration
Custom DNS Suffixes
Network Adapters
vmnic0 (00:0c:29:52:b0:81)
The adapters listed here provide the default network connection to and from this host. When two or more adapters are used, connections will be fault-tolerant and outgoing traffic will be load-balanced.
<Up/Down> Select
<Enter> Change
<Esc> Exit
VMware ESXi 5.1.0 (VMkernel Release Build 799733)

Abb. 17: Untermenü zur Konfiguration des „Management Networks“

Markieren Sie durch Drücken der Leertaste diejenige Netzwerkkarte, die den Status „*Connected*“ hat mit einem „*X*“. Entfernen Sie eventuell gesetzte Markierungen bei den anderen Netzwerkkarten. Bestätigen mit Enter.

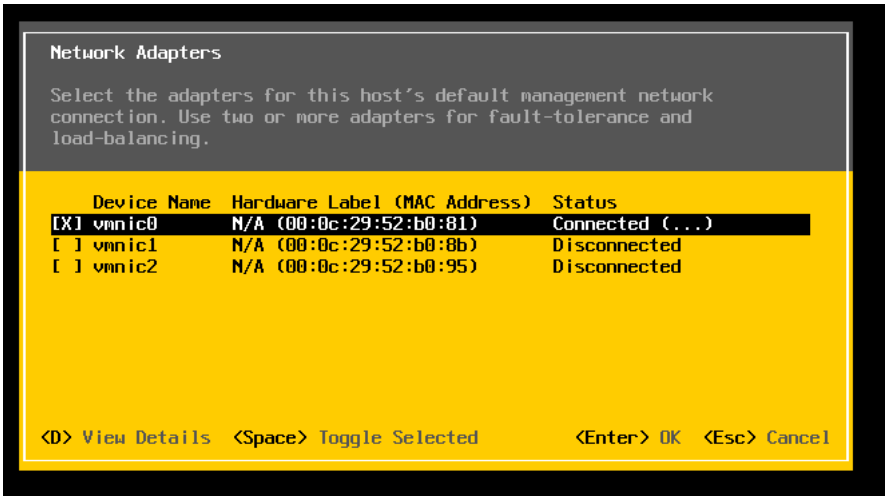

Network Adapters
Select the adapters for this host's default management network connection. Use two or more adapters for fault-tolerance and load-balancing.
Device Name Hardware Label (MAC Address) Status
[X] vmnic0 N/A (00:0c:29:52:b0:81) Connected (...)
[ ] vmnic1 N/A (00:0c:29:52:b0:8b) Disconnected
[ ] vmnic2 N/A (00:0c:29:52:b0:95) Disconnected
<D> View Details <Space> Toggle Selected <Enter> OK <Esc> Cancel

Abb. 18: Konfiguration der Netzwerkkarte für das „Management Network“

2.6.3 Setzen der IP-Adresse im „Management-Network“

Zurück im nachfolgenden Menü wählen Sie bitte per Pfeiltaste die Option „*IP Configuration*“ aus und bestätigen Sie dann die Auswahl mit Enter:

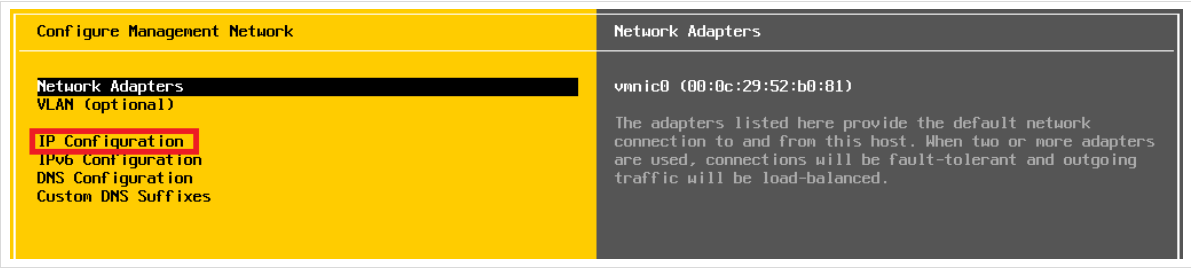

Configure Management Network
Network Adapters
VLAN (optional)
IP Configuration
IPv6 Configuration
DNS Configuration
Custom DNS Suffixes
Network Adapters
vmnic0 (00:0c:29:52:b0:81)
The adapters listed here provide the default network connection to and from this host. When two or more adapters are used, connections will be fault-tolerant and outgoing traffic will be load-balanced.

Abb. 19: Auswahl des Punkts „IP Configuration“

Wählen Sie die zweite Option („*Set static IP address…*“) aus. Vergeben Sie die statische IP (ggf. auf eigenen IP-Bereich anpassen!) und bestätigen Sie mit Enter.

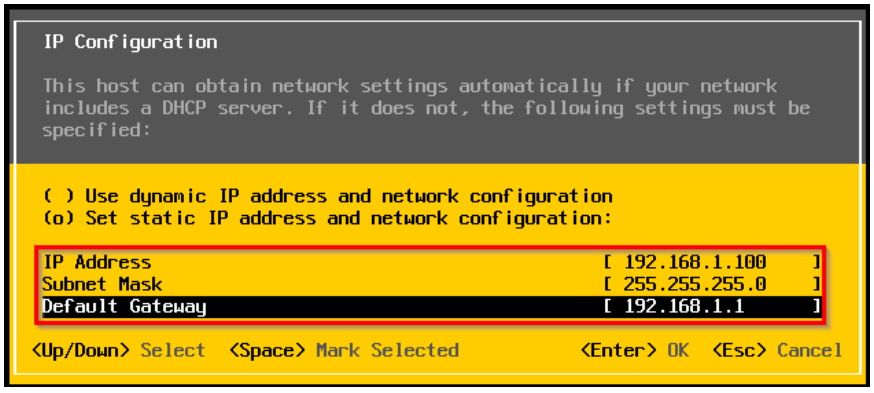

IP Configuration
This host can obtain network settings automatically if your network includes a DHCP server. If it does not, the following settings must be specified:
( ) Use dynamic IP address and network configuration
(o) Set static IP address and network configuration:
IP Address [192.168.1.100]
Subnet Mask [255.255.255.0]
Default Gateway [192.168.1.1]
<Up/Down> Select <Space> Mark Selected <Enter> OK <Esc> Cancel

Abb. 20: Eintragen der statischen IP-Adresse

2.6.4 Deaktivieren von IPv6

Die Deaktivierung von IPv6 auf dem Hypervisor ist nicht zwingend erforderlich, wird jedoch empfohlen.

Wählen Sie im Konfigurationsmenü per Pfeiltaste die Option „*IPv6 Configuration*“ aus und bestätigen Sie dann die Auswahl mit Enter:

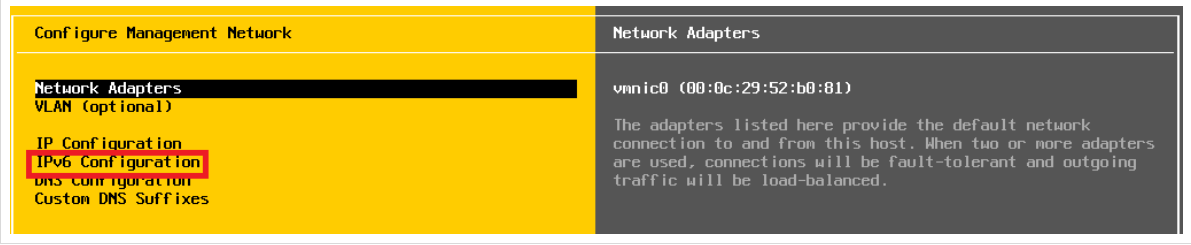

Configure Management Network
Network Adapters
VLAN (optional)
IP Configuration
IPv6 Configuration
DNS Configuration
Custom DNS Suffixes
Network Adapters
vmnic0 (00:0c:29:52:b0:81)
The adapters listed here provide the default network connection to and from this host. When two or more adapters are used, connections will be fault-tolerant and outgoing traffic will be load-balanced.

Abb. 21: Navigation zur Konfiguration von IPv6

Um IPv6 zu deaktivieren, muss das Kreuz bei „*Enable IPv6*“ entfernt werden. Bestätigen Sie dann die Auswahl mit Enter.

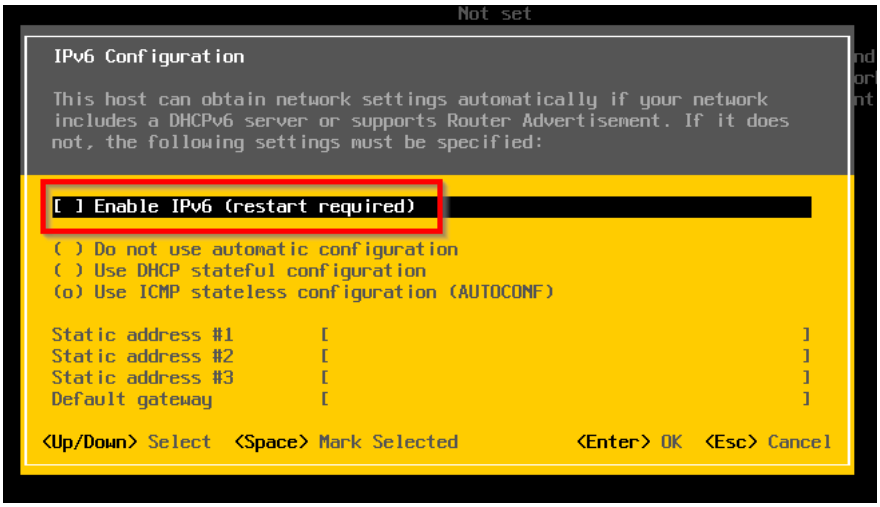

Not set
IPv6 Configuration
This host can obtain network settings automatically if your network includes a DHCPv6 server or supports Router Advertisement. If it does not, the following settings must be specified:
[ ] Enable IPv6 (restart required)
( ) Do not use automatic configuration
( ) Use DHCP stateful configuration
(o) Use ICMP stateless configuration (AUTOCONF)
Static address #1 [ ]
Static address #2 [ ]
Static address #3 [ ]
Default gateway [ ]
<Up/Down> Select <Space> Mark Selected <Enter> OK <Esc> Cancel

Abb. 22: Deaktivieren von IPv6: Kreuz entfernen

2.6.5 Konfigurieren von DNS und Hostname

Die Namensauflösung per DNS muss auf dem Virtualisierungs-Host unbedingt funktionieren, da davon weitere Dienste wie z.B. die Zeitsynchronisation aller virtuellen Maschinen abhängen!

Zurück im nachfolgend dargestellten Menü wählen Sie bitte per Pfeiltaste die Option „*DNS Configuration*“ aus. Bestätigen Sie die Auswahl mit Enter:

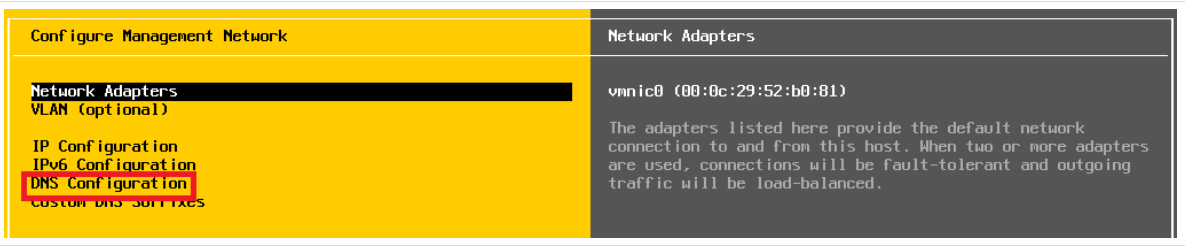

Configure Management Network
Network Adapters
VLAN (optional)
IP Configuration
IPv6 Configuration
DNS Configuration
Network Adapters
vmnic0 (00:0c:29:52:b0:81)
The adapters listed here provide the default network connection to and from this host. When two or more adapters are used, connections will be fault-tolerant and outgoing traffic will be load-balanced.

Abb. 23: Zur Konfiguration von DNS und Hostname

Wählen Sie die zweite Option („*Use the following DNS server addresses and hostname:*“) aus.

Tragen Sie zwei gültige DNS-Server ein. Die genauen Adressen hängen von der konkreten Netzkonfiguration in der Schule ab, denkbare DNS-Server sind:

- Die (interne) IP-Adresse ihres Internetzugangsrouters, falls auf diesem ein eigener DNS-Server läuft. Dies könnte z.B. *192.168.178.1* sein.
- Der DNS-Server, den Sie von ihrem Internetanbieter genannt bekommen. Im Falle eines BelWü-Zugangs ist dies dann z.B. *129.143.2.1* oder *129.143.2.4*.
- Einen öffentlich zugänglichen DNS-Server, z.B. die von Google betriebenen DNS-Server *8.8.8.8 und 8.8.4.4.*

Benennen Sie den Virtualisierungs-Host wie beispielhaft dargestellt. Bestätigen Sie mit Enter:

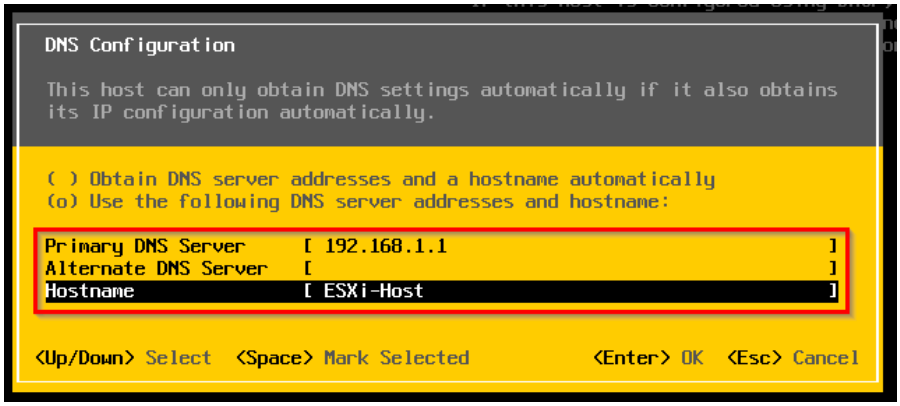

DNS Configuration
This host can only obtain DNS settings automatically if it also obtains its IP configuration automatically.
( ) Obtain DNS server addresses and a hostname automatically
(o) Use the following DNS server addresses and hostname:
Primary DNS Server [192.168.1.1]
Alternate DNS Server [ ]
Hostname [ESXi-Host]
<Up/Down> Select <Space> Mark Selected <Enter> OK <Esc> Cancel

Abb. 24: Konfiguration von DNS und Hostname

2.6.6 Durchführen der Änderungen und Neustart des Virtualisierungs-Hosts

Verlassen Sie das Untermenü „*Configure Management Network*“ durch Drücken von ESC. Im nachfolgenden Fenster werden Sie aufgefordert, die Änderungen am Virtualisierungs-Host zu bestätigen. Bestätigen Sie die Änderungen durch Drücken der Taste Y:

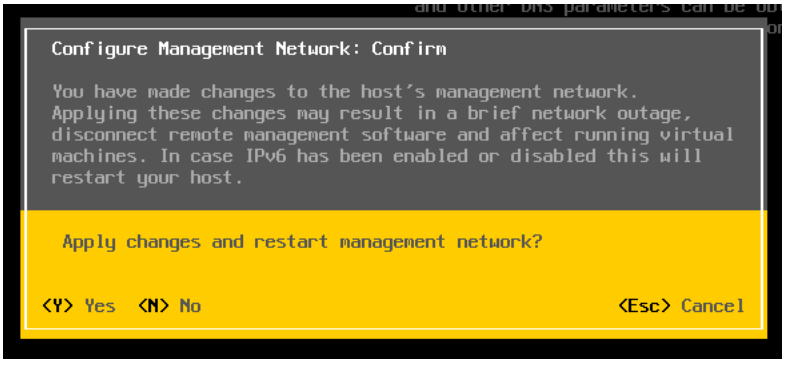

Configure Management Network: Confirm
You have made changes to the host's management network. Applying these changes may result in a brief network outage, disconnect remote management software and affect running virtual machines. In case IPv6 has been enabled or disabled this will restart your host.
Apply changes and restart management network?
<Y> Yes <N> No <Esc> Cancel

Abb. 25: Endgültige Bestätigung der Änderungen am „Management Network“

Im Anschluss wird ein Neustart des Virtualisierungs-Hosts durchgeführt:

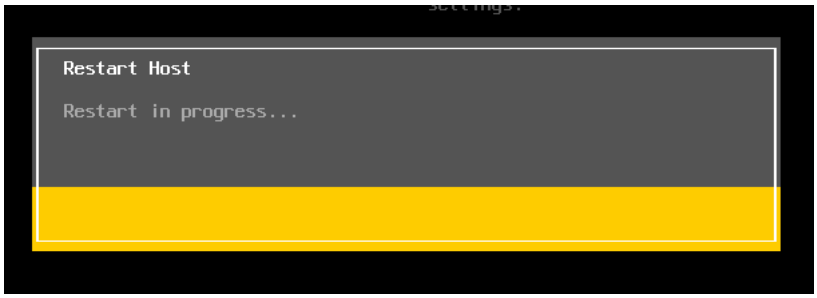


Abb. 26: Neustart des Virtualisierungs-Hosts

Nach dem Neustart ist die Netzwerkkarte im Netz „*INTERNET*“ für das Management des Virtualisierungs-Hosts eingerichtet. Auf der Startseite des Virtualisierungs-Hosts sollten die eben eingestellte IP-Adresse und der Hostname angezeigt werden:

VMware ESXi 5.1.0 (VMKernel Release Build 1065491)
VMware, Inc. VMware Virtual Platform
Intel(R) Core(TM) i7-2760QM CPU @ 2.40GHz
13 GiB Memory
Download tools to manage this host from:
http://ESXi-Host/
http://192.168.1.100/ (STATIC)
<F2> Customize System/View Logs
<F12> Shut Down/Restart

Abb. 27: Startseite nach erfolgtem Reboot

2.6.7 Test der DNS-Namensauflösung

Melden Sie sich auf der Konsole des Virtualisierungs-Hosts (F2-Taste und anschließende Authentifizierung als Benutzer „*root*“) an und navigieren Sie mit den Pfeiltasten zum Punkt „*Test Management Network*“ und drücken Sie Enter.

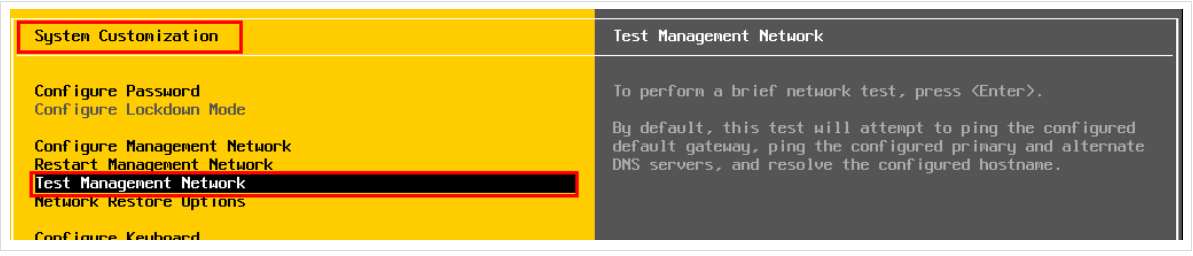

System Customization
Configure Password
Configure Lockdown Mode
Configure Management Network
Restart Management Network
Test Management Network
Network Restore Options
Configure Keyboard
Test Management Network
To perform a brief network test, press <Enter>.
By default, this test will attempt to ping the configured default gateway, ping the configured primary and alternate DNS servers, and resolve the configured hostname.

Abb. 28: Diagnosefunktionen des Hypervisors aufrufen

Mit der folgenden Maske können Sie IP-Adressen pingen und die DNS-Namensauflösung testen.

Tragen Sie einen externen Hostnamen in das letzte Feld ein (z.B. „www.lmz-bw.de“) und starten Sie den Test mit Klick auf Enter:

Test Management Network
By default, this test will attempt to ping your default gateway and DNS servers, and resolve your hostname.
Ping Address #0: [ ]
Ping Address #1: [ ]
Ping Address #2: [ ]
Resolve Hostname [www.lmz-bw.de]
<Up/Down> Select
<Enter> OK
<Esc> Cancel

Abb. 29: Test der DNS-Namensauflösung

Eine erfolgreiche Namensauflösung wird mit „*OK*“ quittiert. Schlägt die Namensauflösung fehl (Meldung „*Failed*“), muss die Netzkonfiguration nochmals überprüft werden.

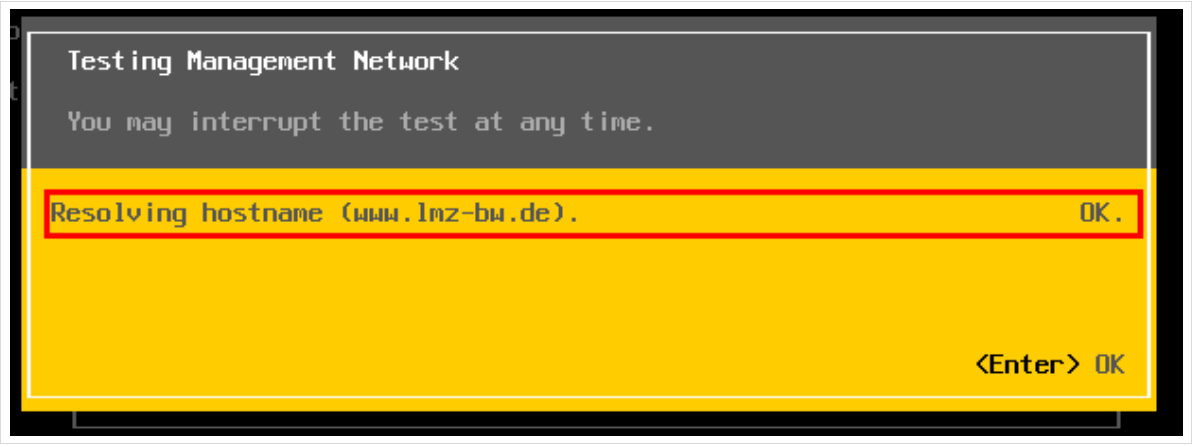


Abb. 30: Erfolgreiche Namensauflösung.

2.6.8 Test der Erreichbarkeit des Virtualisierungs-Hosts

Wenn die vorherigen Schritte korrekt ausgeführt worden sind, ist der Virtualisierungs-Host aus dem Netz „*INTERNET*“ zu erreichen.

- Schließen Sie für den Test den Management-PC an das Netz „*INTERNET*“ an.
- Vergeben Sie für diesem Rechner manuell eine IP-Adresse aus dem Netzbereich des Netzes „*INTERNET*“ (im obigen Beispiel z.B. *192.168.1.101*) und setzen Sie dessen Netzwerkmaske korrekt (im obigen Beispiel auf *255.255.255.0*).
- Öffnen Sie einen Browser auf dem Management-PC.
- Geben Sie in die Adresszeile des Browsers die IP-Adresse des Hypervisors ein (in unserem Beispiel http://192.168.1.100).

- Daraufhin sollten Sie das folgende Bild sehen:

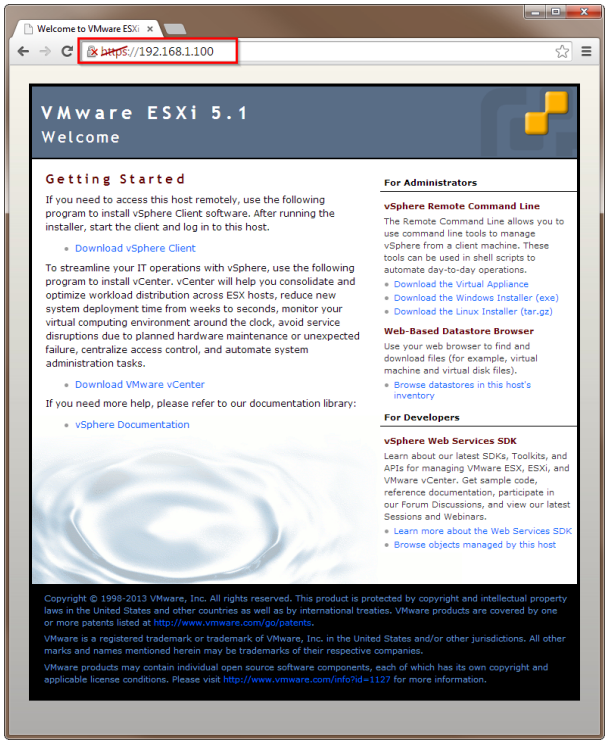

Welcome to VMware ESXi
https://192.168.1.100
VMware ESXi 5.1
Welcome
Getting Started
If you need to access this host remotely, use the following program to install vSphere Client software. After running the installer, start the client and log in to this host.
Download vSphere Client
To streamline your IT operations with vSphere, use the following program to install vCenter. vCenter will help you consolidate and optimize workload distribution across ESX hosts, reduce new system deployment time from weeks to seconds, monitor your virtual computing environment around the clock, avoid service disruptions due to planned hardware maintenance or unexpected failure, centralize access control, and automate system administration tasks.
Download VMware vCenter
If you need more help, please refer to our documentation library:
vSphere Documentation
For Administrators
vSphere Remote Command Line
The Remote Command Line allows you to use command line tools to manage vSphere from a client machine. These tools can be used in shell scripts to automate day-to-day operations.
Download the Virtual Appliance
Download the Windows Installer (exe)
Download the Linux Installer (tar.gz)
Web-Based Datastore Browser
Use your web browser to find and download files (for example, virtual machine and virtual disk files).
Browse datastores in this host's inventory
For Developers
vSphere Web Services SDK
Learn about our latest SDKs, Toolkits, and APIs for managing VMware ESX, ESXi, and VMware vCenter. Get sample code, reference documentation, participate in our Forum Discussions, and view our latest Sessions and Webinars.
Learn more about the Web Services SDK
Browse objects managed by this host
Copyright © 1998-2013 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.
VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.
VMware products may contain individual open source software components, each of which has its own copyright and applicable license conditions. Please visit http://www.vmware.com/info?id=1127 for more information.

Abb. 31: Test des Zugriffs auf den Virtualisierungs-Host, IP-Adresse ist auf eigene Konfiguration anzupassen!

Wenn Sie diese Seite im Browser sehen, können Sie mit den nächsten Schritten fortfahren. Andernfalls muss die Netzwerkkonfiguration überprüft werden.

2.7 Installation des vSphere-Clients

Die fortgeschrittene Konfiguration des bisher eingerichteten Virtualisierungs-Hosts wird mit dem *vSphere-Client*, einem grafischen Werkzeug aus dem Hause *VMware*, durchgeführt. Für die folgenden Schritte muss der Management-PC mit dem Netz „*INTERNET*“ verbunden sein.

Sollten Sie die Installationsdateien für den vSphere-Client bereits heruntergeladen haben, können Sie gleich zum Abschnitt „*Installation des vSphere-Clients*“ (vgl. Kapitel 2.7.2) übergehen.

2.7.1 Downloadmöglichkeit des vSphere-Clients

Melden Sie sich am Management-PC an. Öffnen Sie ein Browser-Fenster und geben Sie die IP des Virtualisierungs-Hosts in die Adresszeile ein. Bestätigen Sie mit Enter. Nach Bestätigung der Sicherheits-Abfrage des jeweiligen Browsers (*Self-Signed-Zertifikat ESXi-Host*), gelangen Sie auf die unten dargestellte Intranet Seite des Virtualisierungs-Hosts mit dem entsprechenden Download-Link.

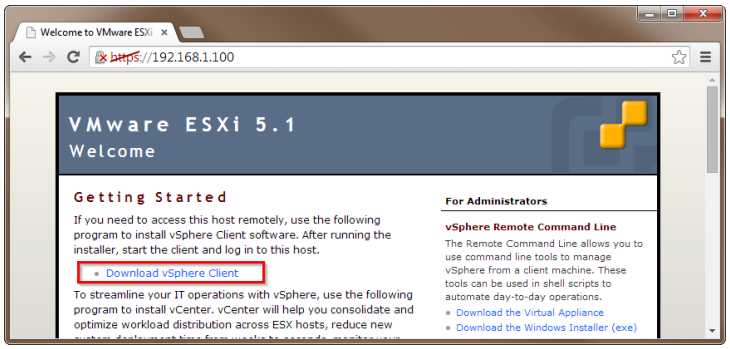

Welcome to VMware ESXi
https://192.168.1.100
VMware ESXi 5.1
Welcome
Getting Started
If you need to access this host remotely, use the following program to install vSphere Client software. After running the installer, start the client and log in to this host.
Download vSphere Client
To streamline your IT operations with vSphere, use the following program to install vCenter. vCenter will help you consolidate and optimize workload distribution across ESX hosts, reduce new
For Administrators
vSphere Remote Command Line
The Remote Command Line allows you to use command line tools to manage vSphere from a client machine. These tools can be used in shell scripts to automate day-to-day operations.
Download the Virtual Appliance
Download the Windows Installer (exe)

Abb. 32: Intranet-Seite des Virtualisierungs-Hosts mit Download-Link zum vSphere-Client

Sollte der Download über diesen Link nicht funktionieren, so müssen Sie die Datei – wie in Kapitel 2.3 (Seite 14) beschrieben – auf einem Rechner mit Internetzugang herunterladen und auf einem externen Datenträger speichern.

2.7.2 Installation des vSphere-Clients

Führen Sie die heruntergeladene Setup-Datei des *vSphere-Clients* auf dem Management-PC aus, um die Installation der Software vornehmen zu können:

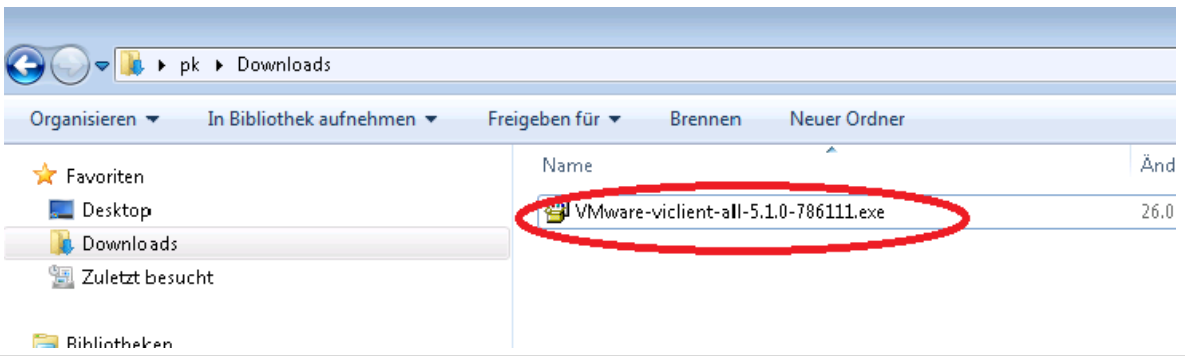


Abb. 33: Installationsdatei des vSphere-Clients

2.7.3 Zugriff vom vSphere-Client auf den Hypervisor

Nach erfolgreicher Installation des *vSphere-Clients* finden Sie, wie unten abgebildet, auf dem Desktop des Management-PCs eine entsprechende Programmverknüpfung vor. Starten Sie hierüber per Doppelklick den *vSphere-Client*:

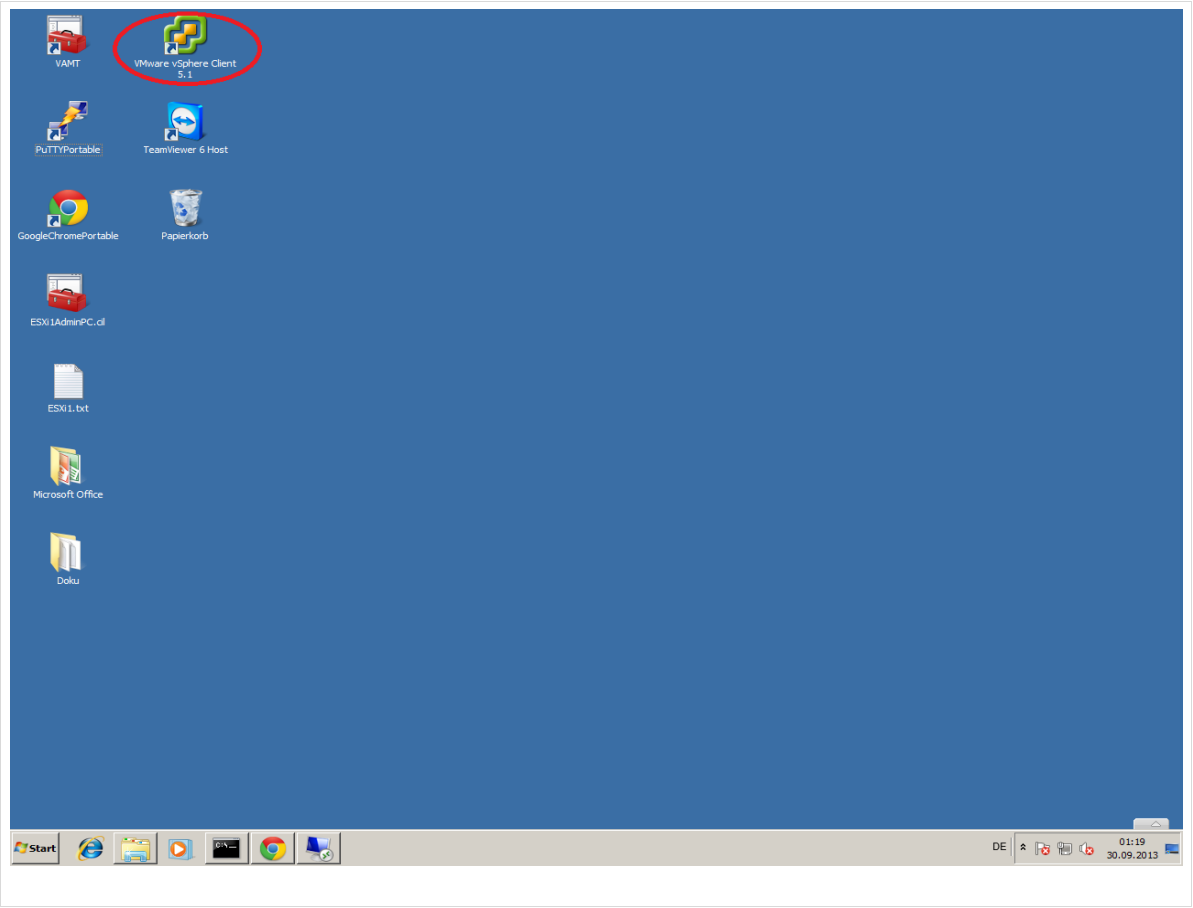


Abb. 34: vSphere-Client ist auf dem Management-PC installiert.

Melden Sie sich mit dem Benutzerkonto *root* und vergebenem Passwort am Virtualisierungs-Host an:

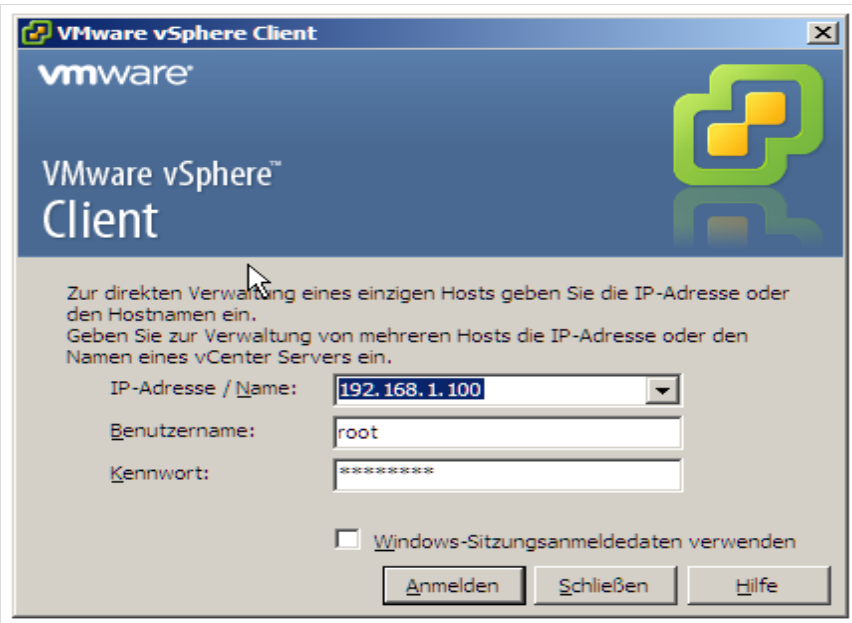


Abb. 35: Anmeldung mit vSphere-Client am Hypervisor

Im nachfolgenden Dialog („*Sicherheitswarnung*“) wählen Sie bitte die im folgenden Screenshot gekennzeichnete Option („*Dieses Zertifikat installieren und keine Sicherheitswarnungen für IP-ADRESSE anzeigen*“) aus, um das SSL-Zertifikat des Hypervisors einmalig auf dem Management-PC zu installieren und klicken Sie auf „*Ignorieren*“.

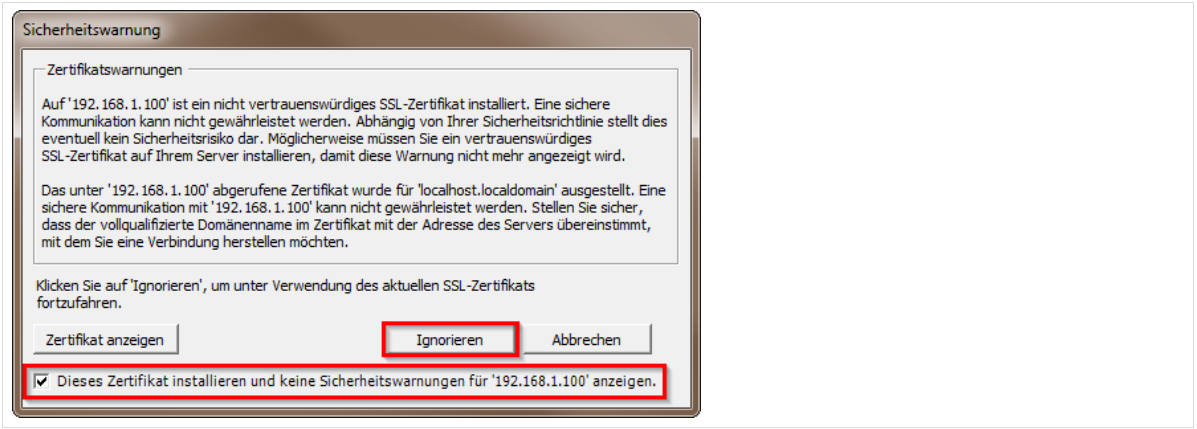

Sicherheitswarnung
Zertifikatswarnungen
Auf '192.168.1.100' ist ein nicht vertrauenswürdiges SSL-Zertifikat installiert. Eine sichere Kommunikation kann nicht gewährleistet werden. Abhängig von Ihrer Sicherheitsrichtlinie stellt dies eventuell kein Sicherheitsrisiko dar. Möglicherweise müssen Sie ein vertrauenswürdiges SSL-Zertifikat auf Ihrem Server installieren, damit diese Warnung nicht mehr angezeigt wird.
Das unter '192.168.1.100' abgerufene Zertifikat wurde für 'localhost.localdomain' ausgestellt. Eine sichere Kommunikation mit '192.168.1.100' kann nicht gewährleistet werden. Stellen Sie sicher, dass der vollqualifizierte Domänenname im Zertifikat mit der Adresse des Servers übereinstimmt, mit dem Sie eine Verbindung herstellen möchten.
Klicken Sie auf 'Ignorieren', um unter Verwendung des aktuellen SSL-Zertifikats fortzufahren.
Zertifikat anzeigen
Ignorieren
Abbrechen
Dieses Zertifikat installieren und keine Sicherheitswarnungen für '192.168.1.100' anzeigen.

Abb. 36: Installieren des SSL-Zertifikats des Hypervisors auf dem Management-PC.

Beim ersten Login zeigt Ihnen der Server den Lizensierungsstatus „*60 Tage Testversion*“ an, bestätigen Sie bitte durch Drücken auf „*OK*“: Damit ist der Zugriff vom vSphere-Client auf den Hypervisor eingerichtet.

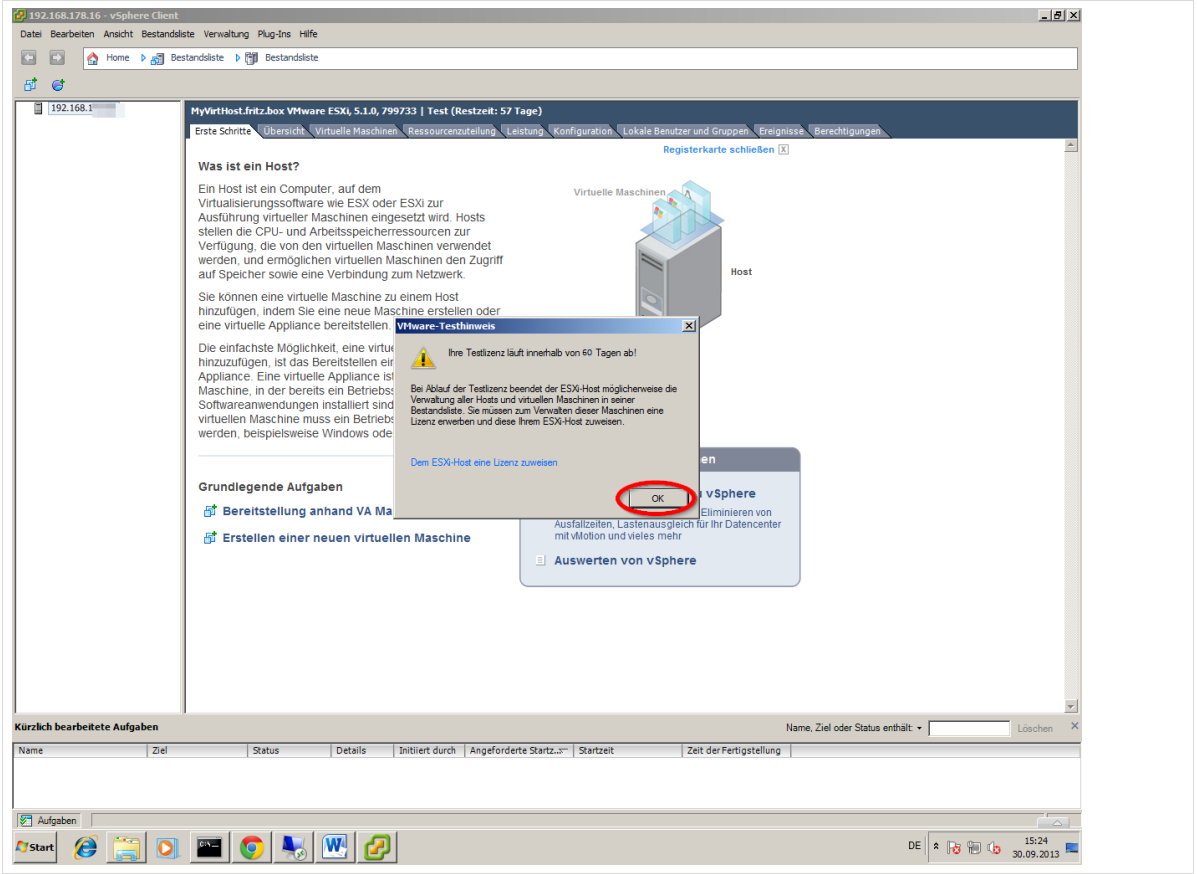

192.168.178.16 - vSphere Client
Datei Bearbeiten Ansicht Bestandsliste Verwaltung Plug-Ins Hilfe
MyVirtHost.fritz.box VMware ESXi, 5.1.0, 799733 | Test (Restzeit: 57 Tage)
Erste Schritte Übersicht Virtuelle Maschinen Ressourcenzuteilung Leistung Konfiguration Lokale Benutzer und Gruppen Ereignisse Berechtigungen
Was ist ein Host?
Ein Host ist ein Computer, auf dem Virtualisierungssoftware wie ESX oder ESXi zur Ausführung virtueller Maschinen eingesetzt wird. Hosts stellen die CPU- und Arbeitsspeicherressourcen zur Verfügung, die von den virtuellen Maschinen verwendet werden, und ermöglichen virtuellen Maschinen den Zugriff auf Speicher sowie eine Verbindung zum Netzwerk.
Virtuelle Maschinen
Host
VMware-Testhinweis
Ihre Testlizenz läuft innerhalb von 60 Tagen ab!
Bei Ablauf der Testlizenz beendet der ESXi-Host möglicherweise die Verwaltung aller Hosts und virtuellen Maschinen in seiner Bestandsliste. Sie müssen zum Verwalten dieser Maschinen eine Lizenz erwerben und diese Ihrem ESXi-Host zuweisen.
Dem ESXi-Host eine Lizenz zuweisen
OK
Grundlegende Aufgaben
Bereitstellung anhand VA Ma
Erstellen einer neuen virtuellen Maschine
vSphere
Eliminieren von Ausfallzeiten, Lastenausgleich für Ihr Datencenter mit vMotion und vieles mehr
Auswerten von vSphere
Kürzlich bearbeitete Aufgaben
Name, Ziel oder Status enthält:
Löschen
Name Ziel Status Details Initiiert durch Angeforderte Startz... Startzeit Zeit der Fertigstellung
Aufgaben
Start
DE
15:24
30.09.2013

Abb. 37: Hinweis auf die 60-Tage-Testversion

2.8 Eingabe des Lizenzschlüssels

Als nächstes muss der Hypervisor lizenziert werden.

Navigieren Sie über die Registerkarte „*Konfiguration*“ (1), das Menü „*Software* | *Lizensierte Funktionen*“ (2) und dort über die Option „*Bearbeiten*“ (3) auf den Dialog für die Eingabe des Lizenzschlüssels:

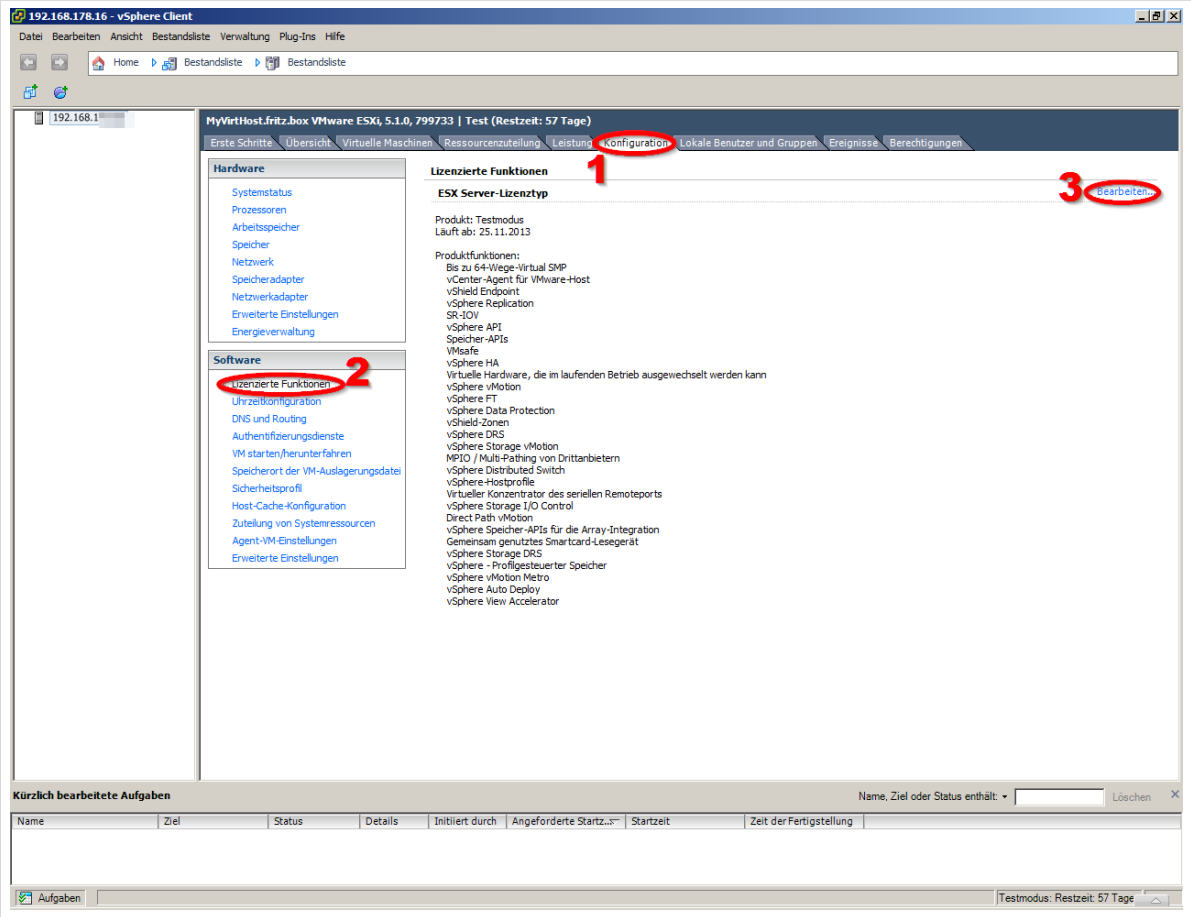


Abb. 38: Zur Eingabe des Lizenzschlüssels

Wählen Sie die Option *„Diesem Host einen neuen Lizenzschlüssel zuweisen“* (1) aus.

Klicken dann den Button *„Schlüssel eingeben…“* (2) und geben dann im darauffolgenden Popup-Fenster *„Lizenzschlüssel hinzufügen“* (3) Ihren individuellen Lizenzschlüssel für den Hypervisor ein.

Bestätigen Sie mit „*OK*“:

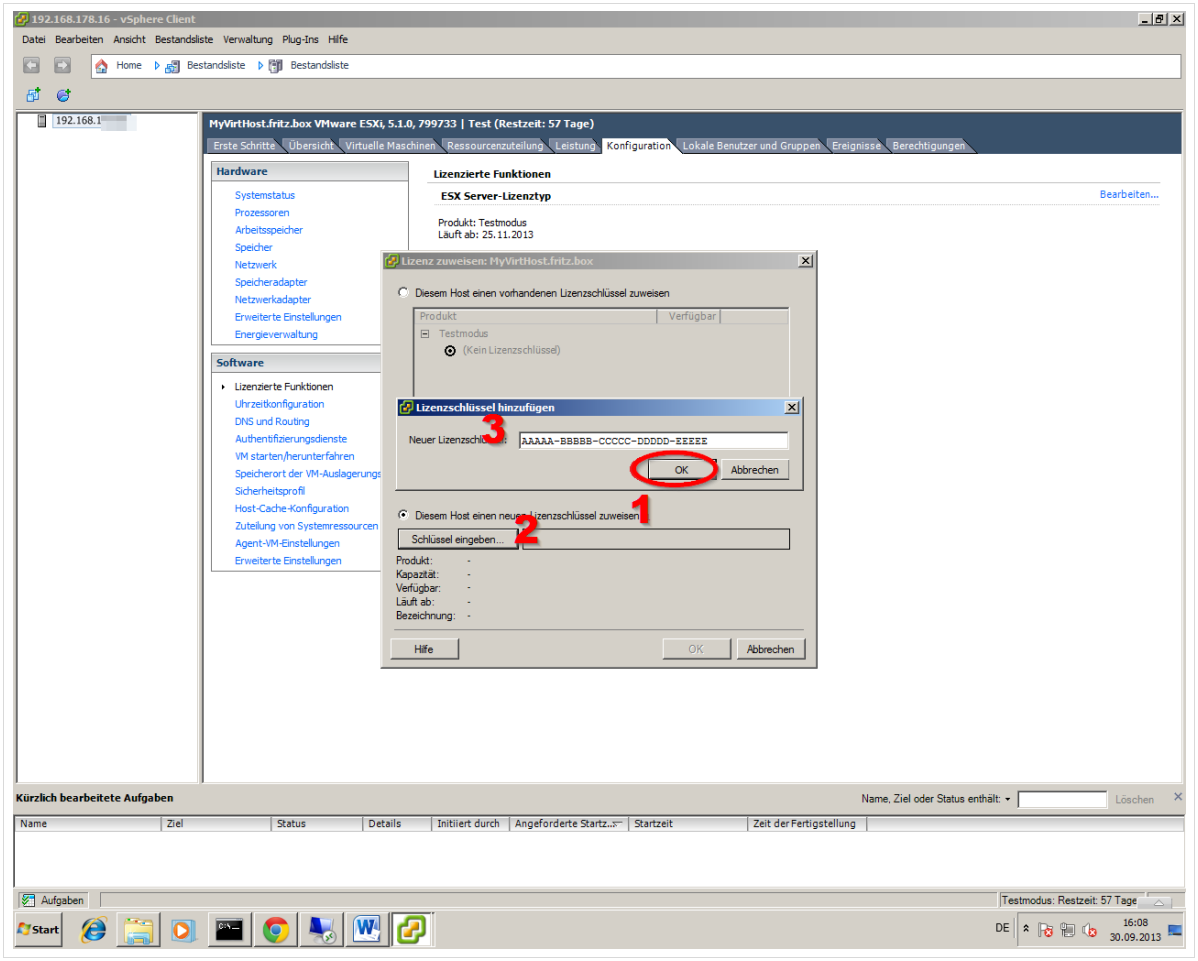


Abb. 39: Eingabe des Lizenzschlüssels für den Hypervisor

Der Lizensierungs-Status Ihres Virtualisierungs-Hosts sollte nun der folgenden Abbildung entsprechen. Eine erfolgreiche Eingabe des Lizenzschlüssels wird mit Einträgen wie „*zeitlich unbegrenzt*“ bzw. „*Läuft ab: Nie*“ im Informationstext des Menü-Eintrages „*Lizensierte Funktionen*“ angezeigt.

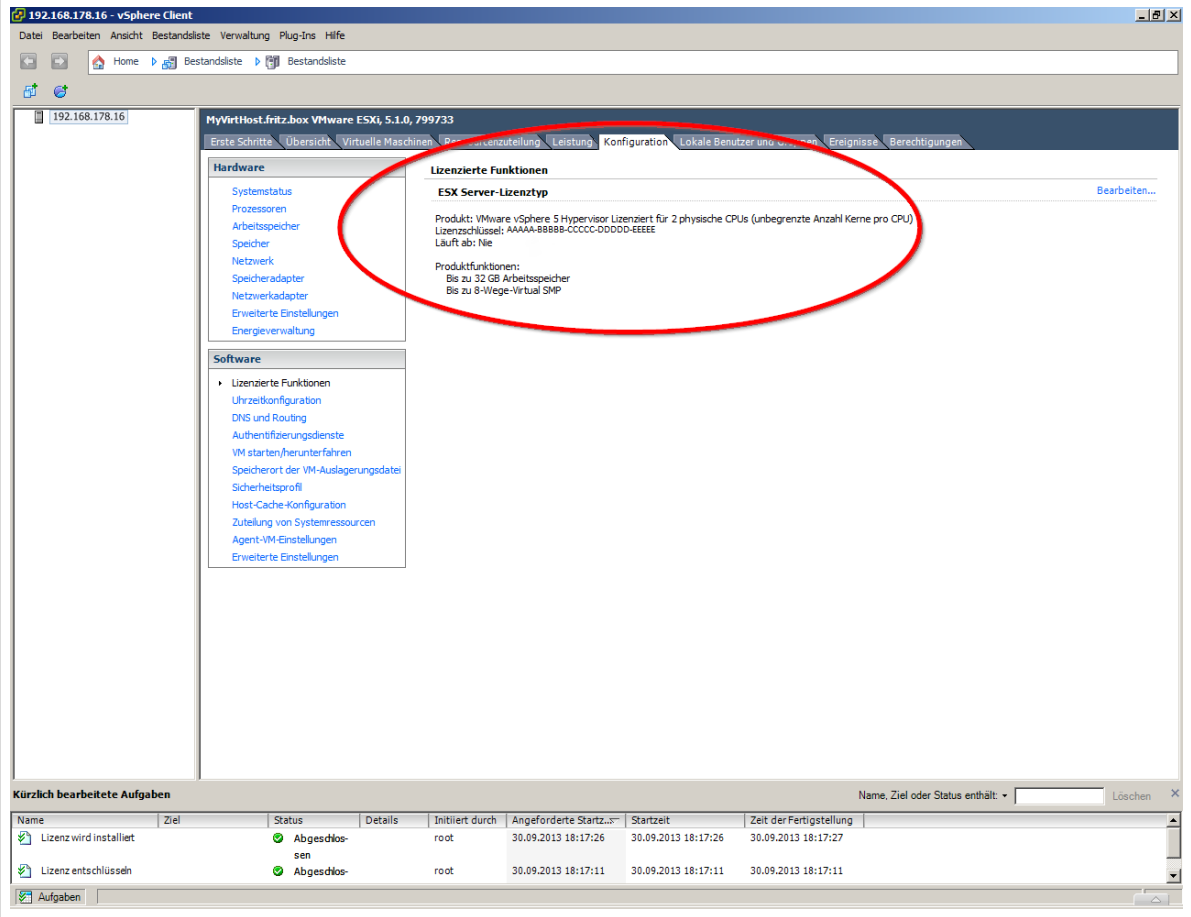


Abb. 40: Lizenzschlüssel wurde korrekt eingetragen

2.9 Zeitsynchronisation des Hypervisors

Im Folgenden wird der Hypervisor so eingerichtet, dass er die Uhrzeit stets mit Zeitservern im Internet per NTP („Network Time Protocol“) abgleicht. Dies ist notwendig, damit die virtuellen Maschinen ihrerseits die korrekte BIOS-Uhrzeit erhalten.

Die Zeitsynchronisation funktioniert nur, wenn das Management-Netz des Hypervisors Internetzugriff hat und die Namensauflösung funktioniert!

Öffnen Sie den vSphere-Client. Wählen Sie im linken Bereich den Hypervisor und öffnen Sie den Reiter „*Konfiguration*“. Wählen Sie im Bereich „*Software*“ die Einstellung „*Uhrzeitkonfiguration*“ aus und klicken Sie rechts oben auf „*Eigenschaften*…“

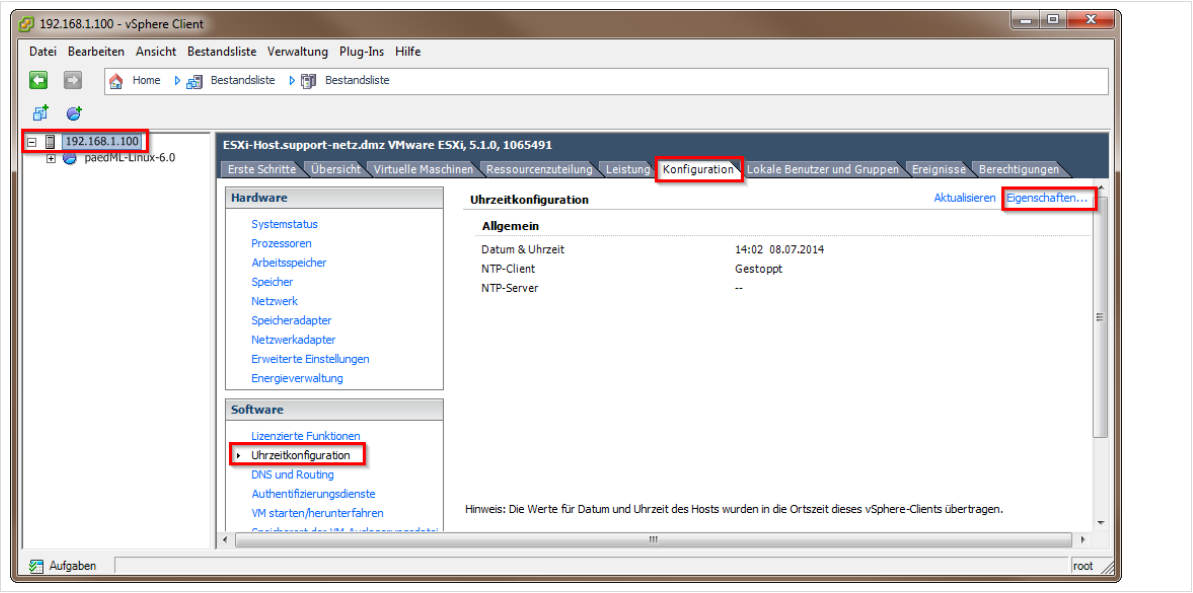


Abb. 41: Ändern der Uhrzeitkonfiguration

Setzen Sie im nächsten Fenster den Haken „*NTP-Client aktiviert*“ und klicken Sie auf „*Optionen…*“

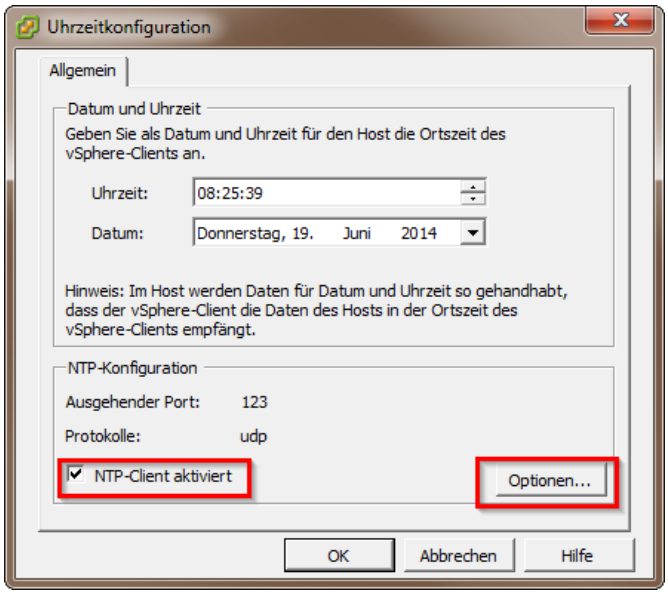

Uhrzeitkonfiguration
Allgemein
Datum und Uhrzeit
Geben Sie als Datum und Uhrzeit für den Host die Ortszeit des vSphere-Clients an.
Uhrzeit: 08:25:39
Datum: Donnerstag, 19. Juni 2014
Hinweis: Im Host werden Daten für Datum und Uhrzeit so gehandhabt, dass der vSphere-Client die Daten des Hosts in der Ortszeit des vSphere-Clients empfängt.
NTP-Konfiguration
Ausgehender Port: 123
Protokolle: udp
NTP-Client aktiviert
Optionen...
OK
Abbrechen
Hilfe

Abb. 42: Aktivieren des NTP-Clients

Wählen Sie im nächsten Fenster in der Kategorie „*Allgemein*“ die Startrichtlinie „*Mit dem Host starten und beenden*“ aus.

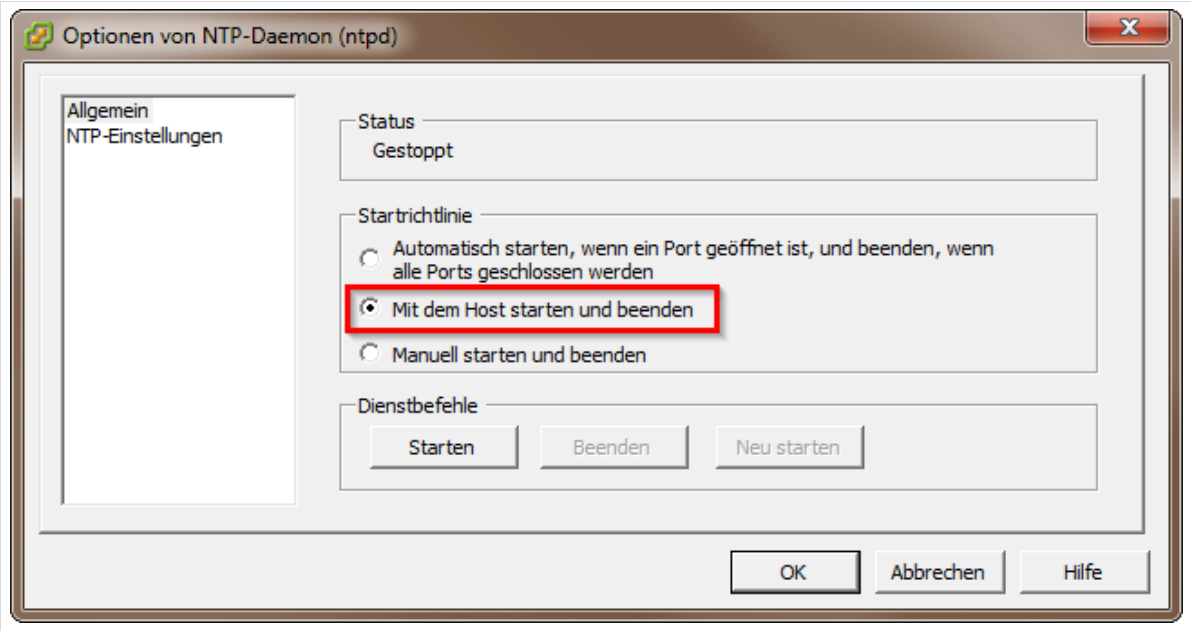


Abb. 43: Festlegen der Startrichtlinie

Klicken Sie nun in die Kategorie „*NTP-Einstellungen*“ und klicken Sie auf „*Hinzufügen…*“, um einen NTP-Server einzutragen.

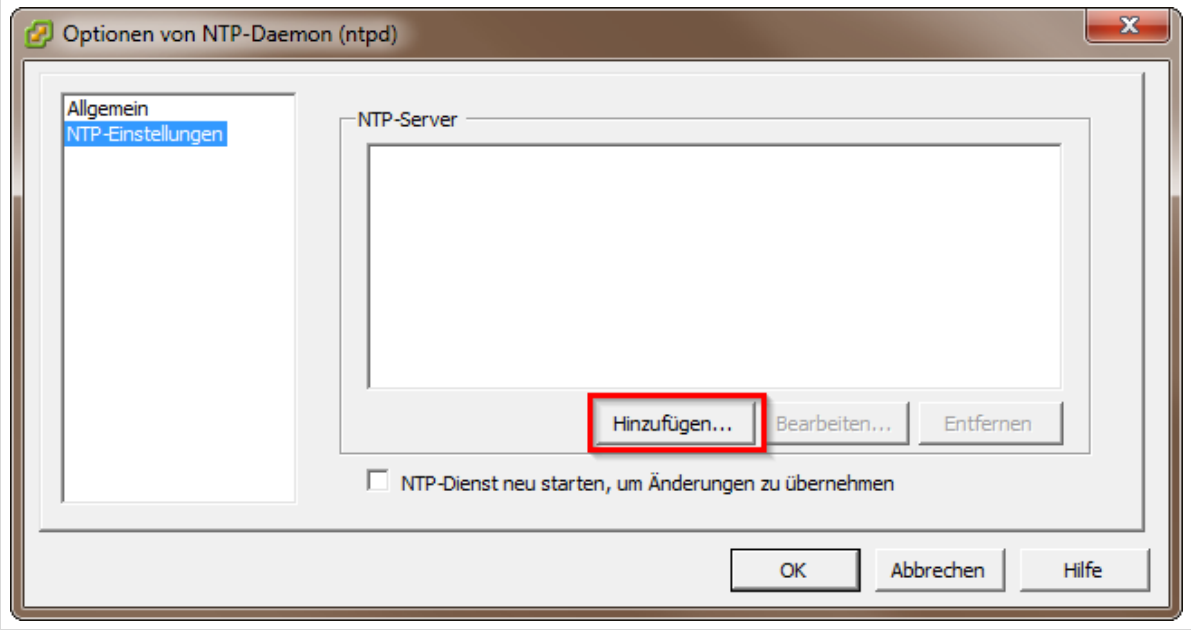


Abb. 44: Hinzufügen von NTP-Servern

Tragen Sie im nächsten Dialog die Zeitserver ein und klicken Sie auf „*OK*“.

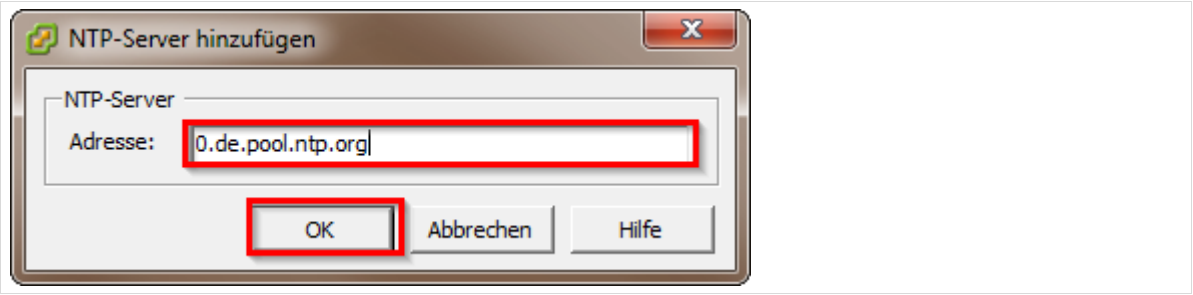


Abb. 45: Eintragen eines Zeitservers.

Es wird empfohlen, nacheinander die folgenden vier Zeitserver hinzuzufügen:

- 0.de.pool.ntp.org
- 1.de.pool.ntp.org
- 2.de.pool.ntp.org
- 3.de.pool.ntp.org

Sind die vier Zeitserver eingetragen, so setzen Sie den Haken „*NTP-Dienst neu starten…“* und klicken Sie auf „*OK*“.

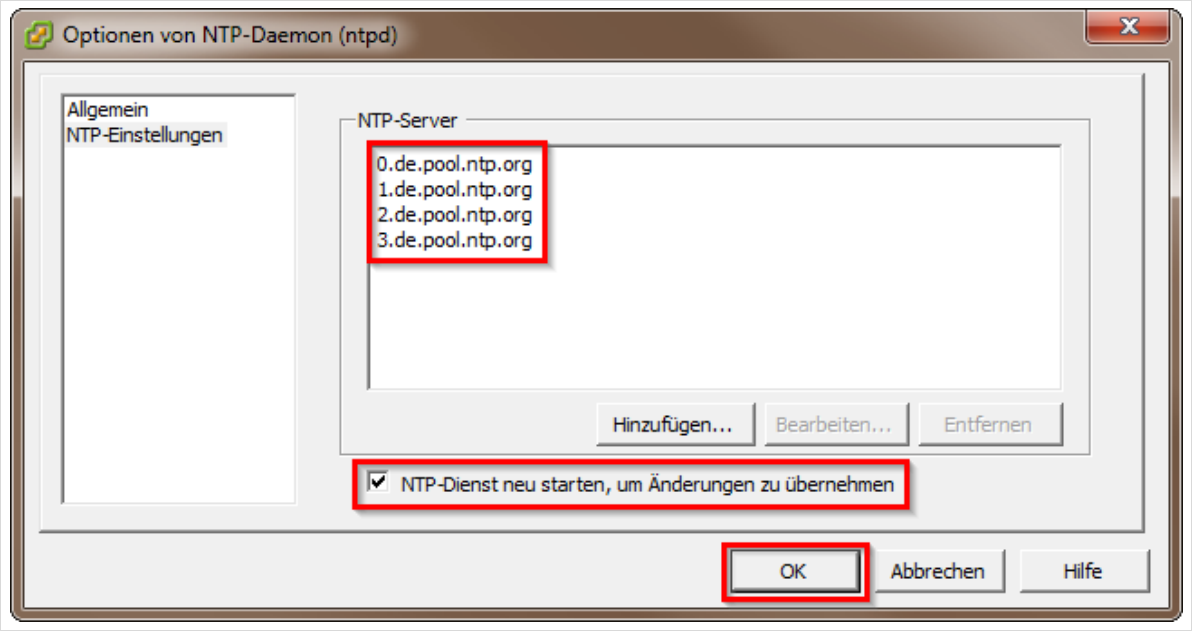


Abb. 46: Übernehmen der Einstellungen und Neustart des NTP-Dienstes.

Zurück in der Uhrzeitkonfiguration tragen Sie einmalig die aktuelle Uhrzeit und das aktuelle Datum im oberen Bereich ein und klicken auf „*OK“*.

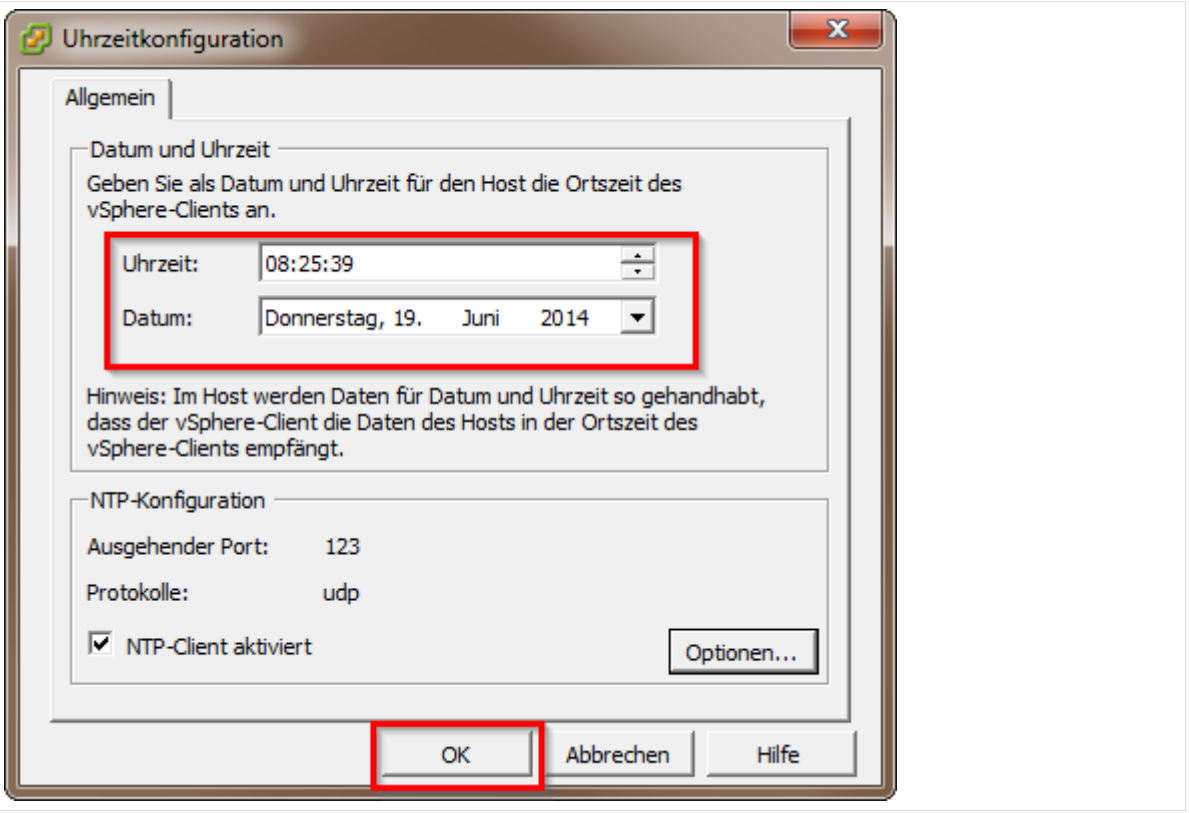


Abb. 47: Eimaliges Eintragen der aktuellen Uhrzeit

Im vSphere-Client sollten Sie nun die folgende Situation vorfinden:

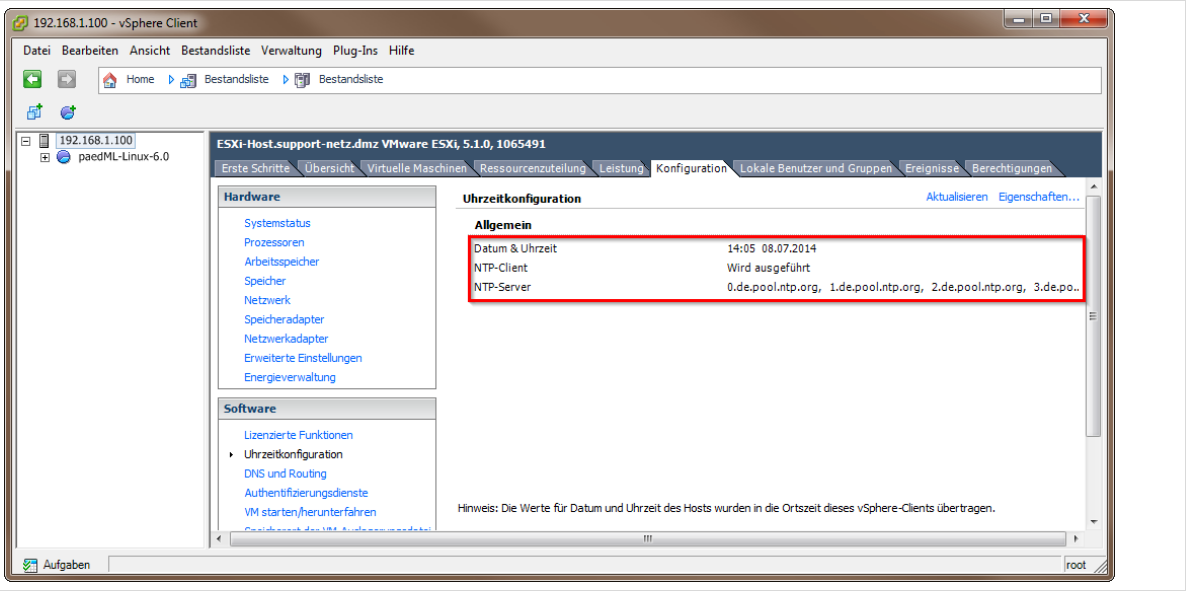


Abb. 48: Der NTP-Client ist erfolgreich eingerichtet.

3. Konfiguration der virtuellen Netzwerke

3.1.1 Definition virtuelles Netzwerk „INTERNET“

Navigieren Sie im *vSphere-Client* über die Registerkarte „*Konfiguration*“ (1) und über die Rubrik „*Netzwerk*“ (2) und wählen Sie dort die Option „*Eigenschaften*“ (3) aus:

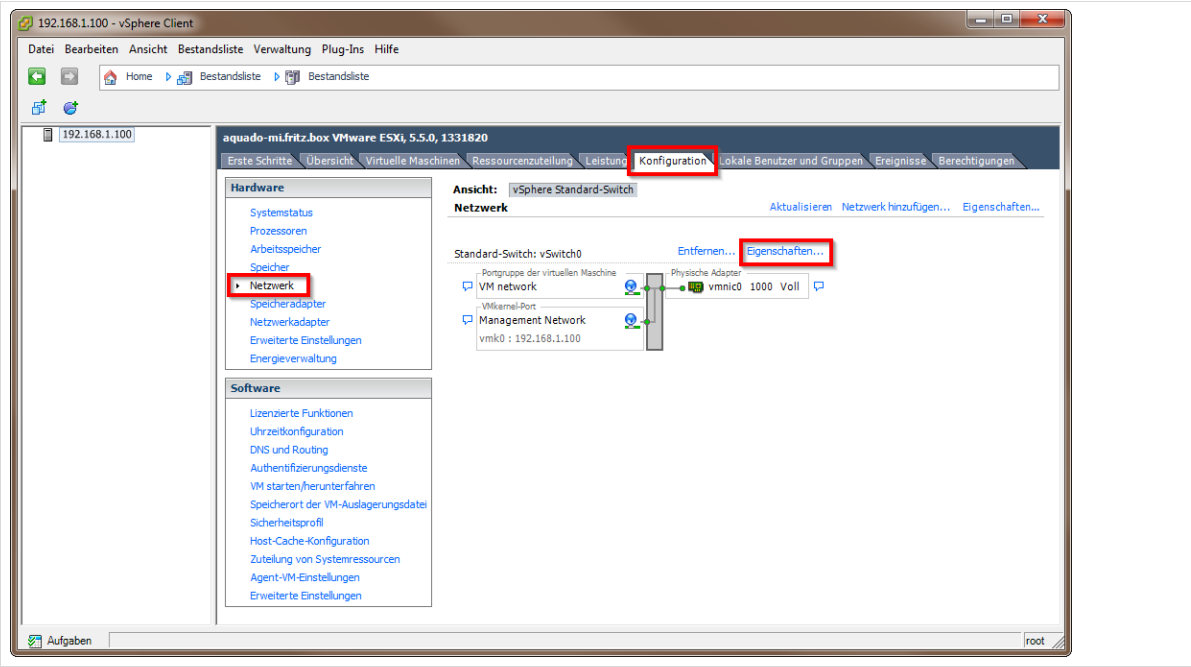


Abb. 49: Konfiguration der Netze auf dem Virtualisierungs-Host

Wählen Sie im Dialog „*vSwitch0-Eigenschaften*“ auf der Registerkarte „*Ports*“ den Eintrag „*VM Network*“ aus und klicken Sie dann den Button „*Bearbeiten*“:

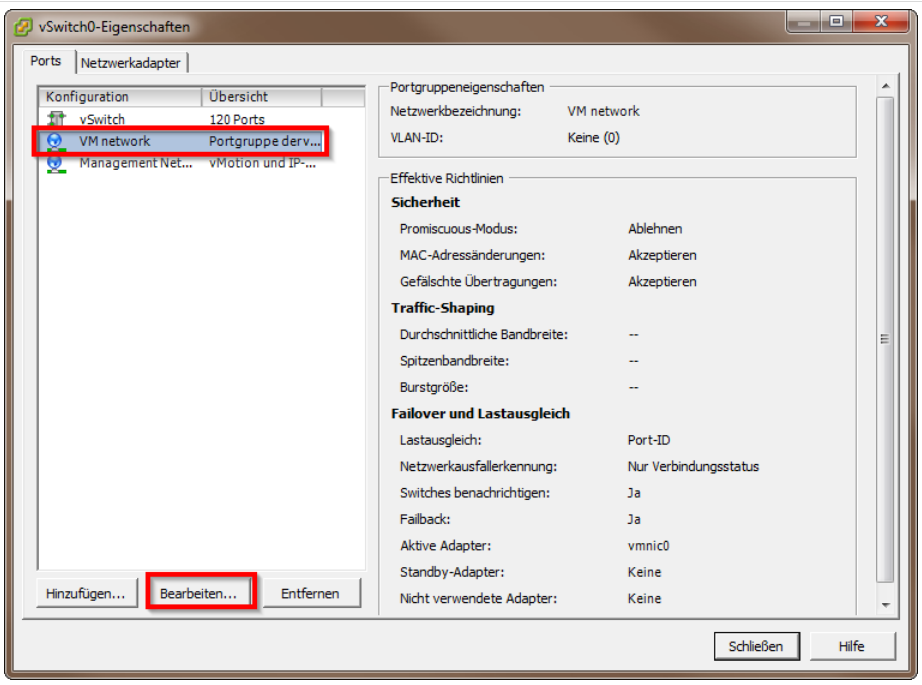


Abb. 50: Bearbeiten von „vSwitch0“

Klicken Sie im Dialog „*VM Network-Eigenschaften*“ in das Feld „*Netzwerkbezeichnung*“. Ändern Sie die Bezeichnung von „*VM Network*“ in „*INTERNET*“ (Großschreibung!) um und bestätigen Sie dann mit „*OK*“:

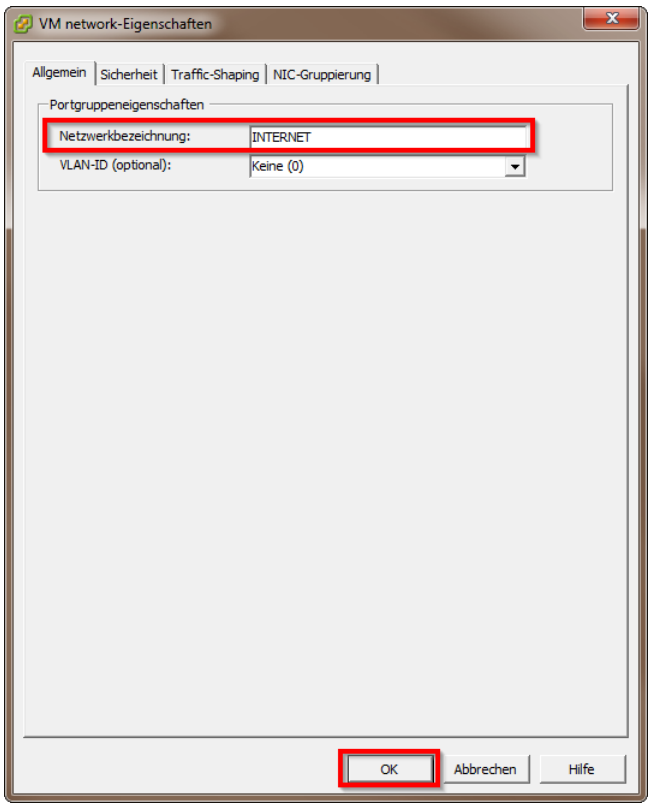


Abb. 51: Umbenennen der Netzwerkbezeichnung in „INTERNET“

Das Ergebnis sollte nun wie folgt aussehen. Bestätigen Sie mit Klick auf „*Schließen*“:

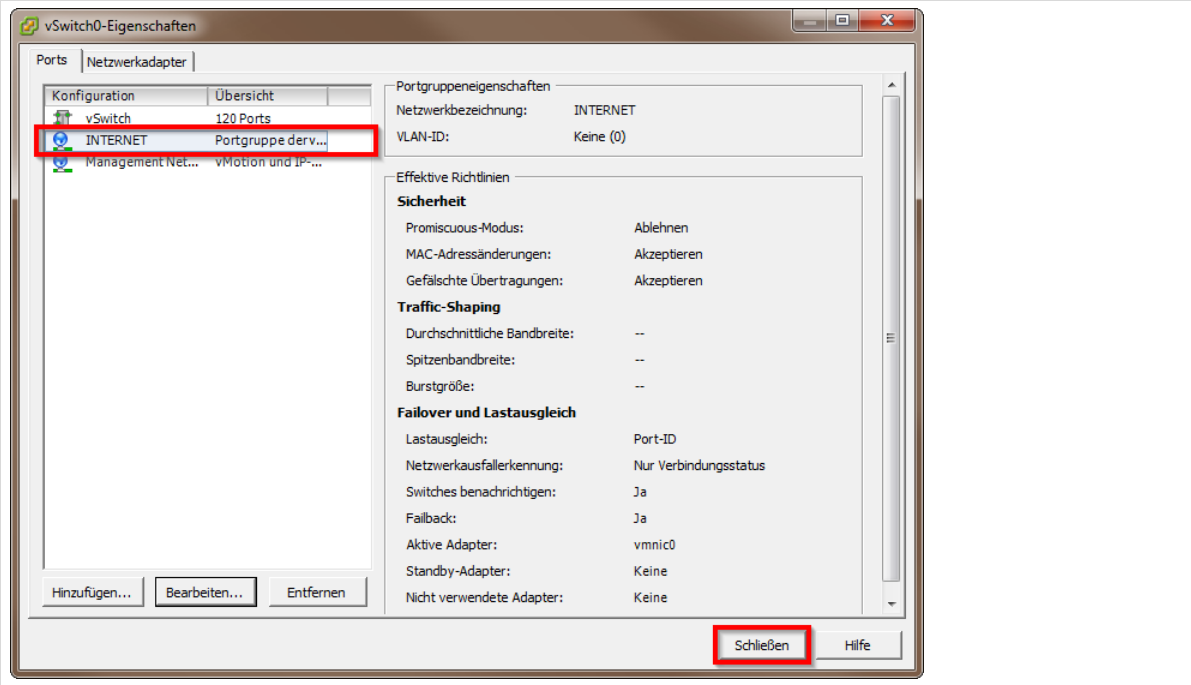


Abb. 52: Das Netzwerk wurde erfolgreich umbenannt.

3.1.2 Definition virtuelles Netzwerk „PAEDAGOGIK“

Navigieren Sie im *vSphere-Client* über die Registerkarte „*Konfiguration*“ (1) und über die Rubrik „*Netzwerk*“ (2) und wählen Sie dort die Option „*Netzwerk hinzufügen*“ (3) aus:

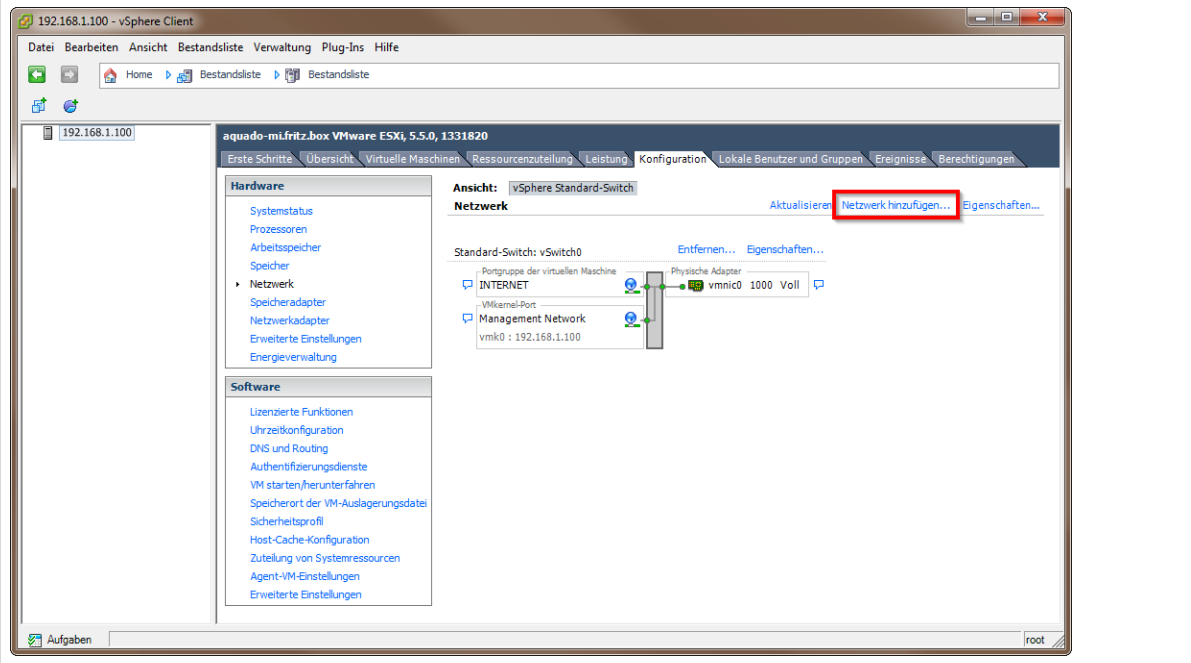


Abb. 53: Hinzufügen eines weiteren Netzwerks

Wählen Sie im folgenden Assistenten die Option „*virtuelle Maschine*“ aus und bestätigen Sie mit Klick auf „*Weiter*“:

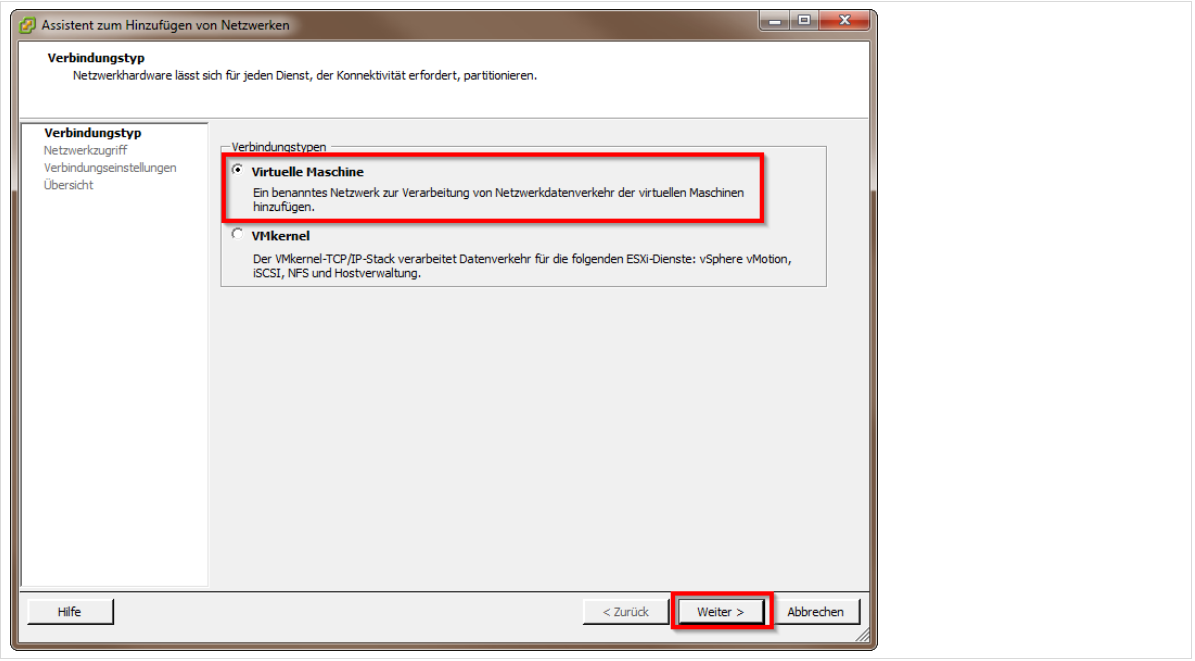


Abb. 54: Verbindungstyp „virtuelle Maschine“ für neues Netzwerk auswählen

Bestätigen Sie die Standardeinstellungen im nächsten Dialog mit „*Weiter*“:

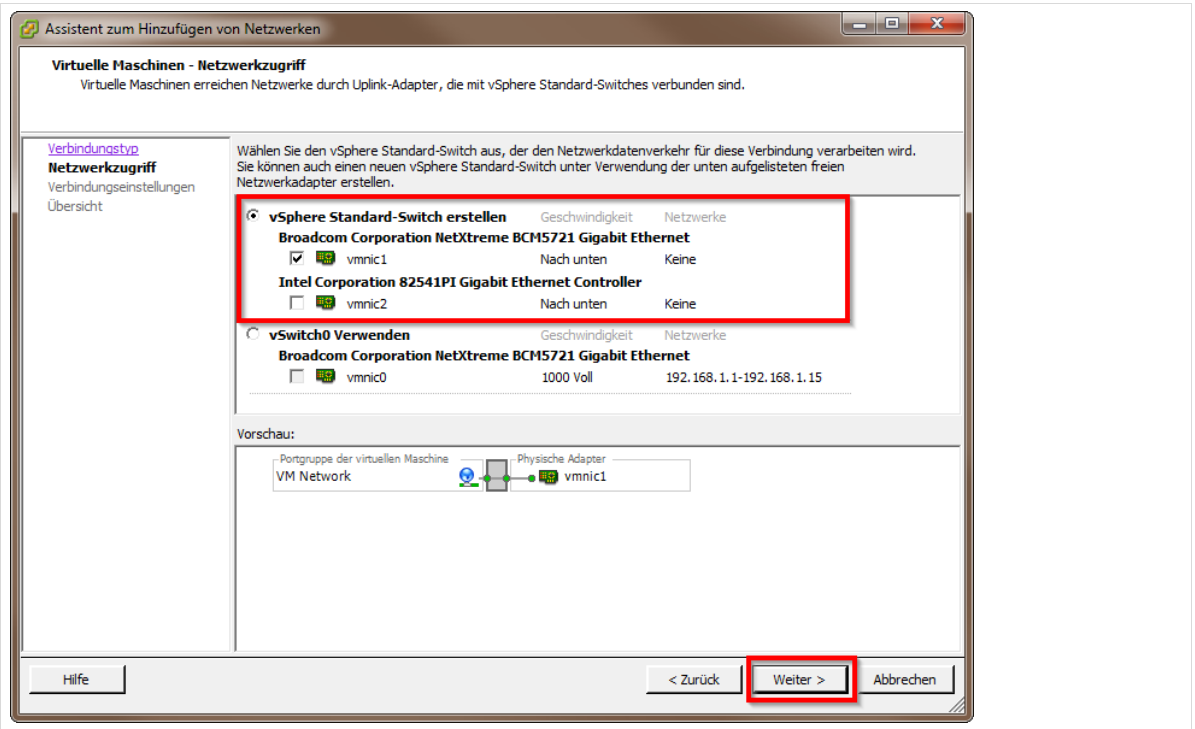


Abb. 55: Standardeinstellungen übernehmen

Geben Sie im folgenden Dialog im Feld „*Netzwerkbezeichnung*“ den Wert „*PAEDAGOGIK*“ (ohne Umlaute, Großschreibung!) ein und bestätigen Sie mit Klick auf „*Weiter*“:

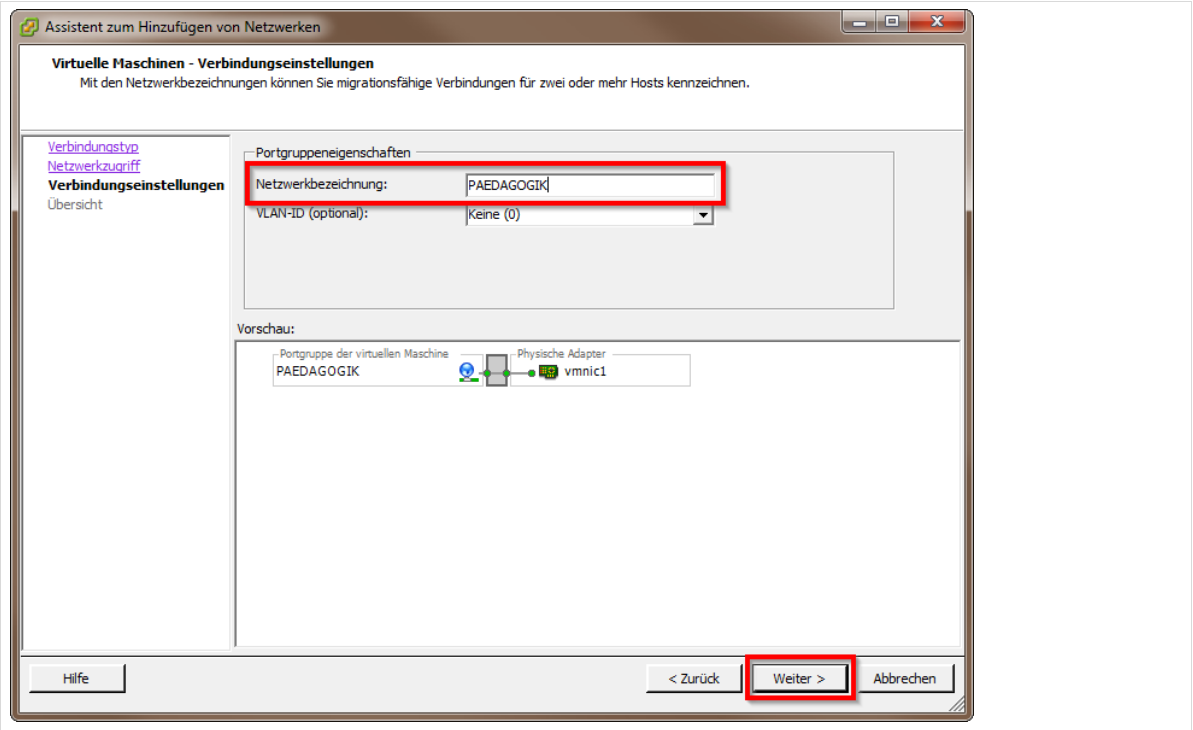


Abb. 56: Bezeichnung „PAEDAGOGIK“ für das neue Netz festlegen

Bestätigen Sie den nachfolgenden Dialog mit Klick auf „*Beenden*“:

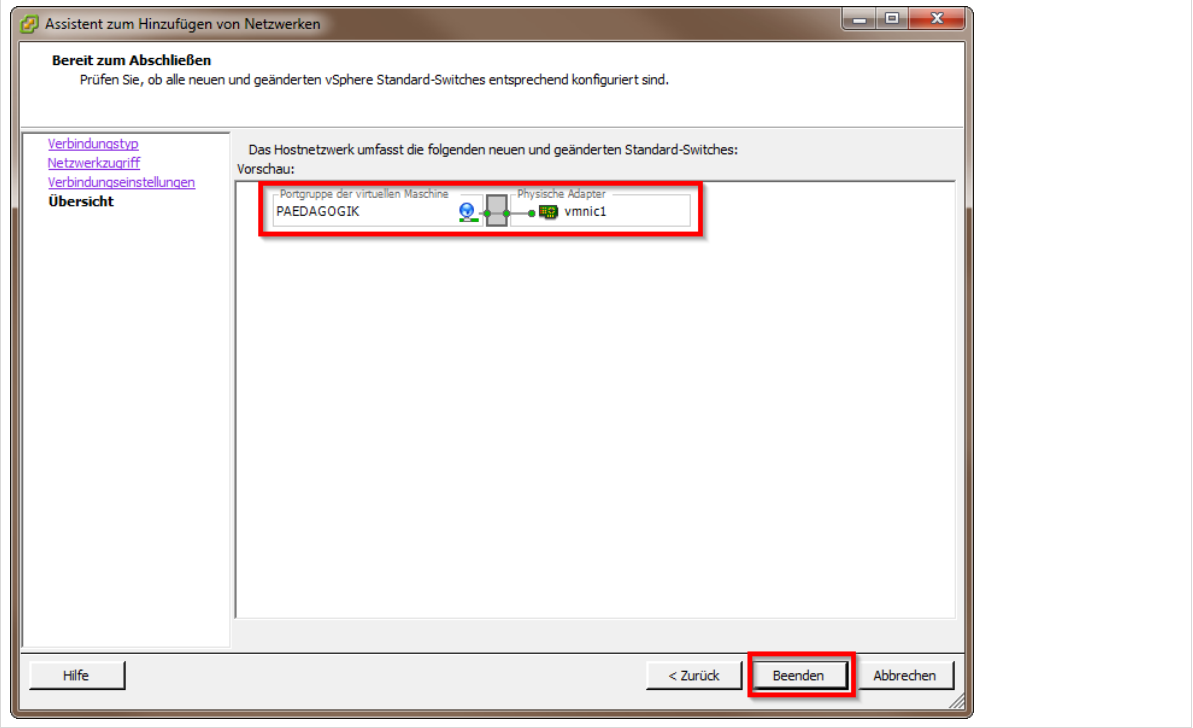


Abb. 57: Einrichten des Netzes „PAEDAGOGIK“ abschließen

3.1.3 Definition virtuelles Netzwerk „GAESTE“

Navigieren Sie im *vSphere-Client* über die Registerkarte „*Konfiguration*“ (1) und über die Rubrik „*Netzwerk*“ (2) und wählen Sie dort die Option „*Netzwerk hinzufügen*“ (3) aus.

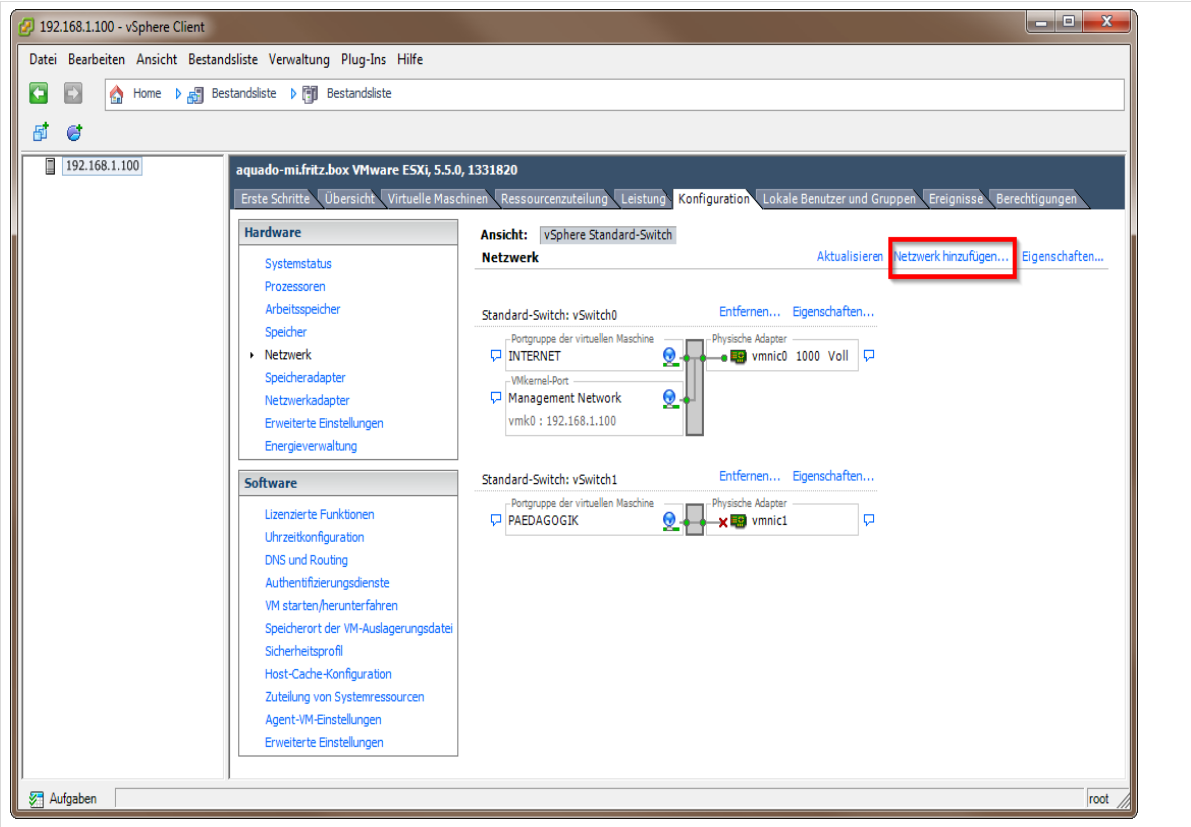


Abb. 58: Hinzufügen eines weiteren virtuellen Netzwerks „GAESTE“

Wählen Sie im folgenden Assistenten die Option „*virtuelle Maschine*“ aus und bestätigen Sie mit Klick auf „*Weiter*“:

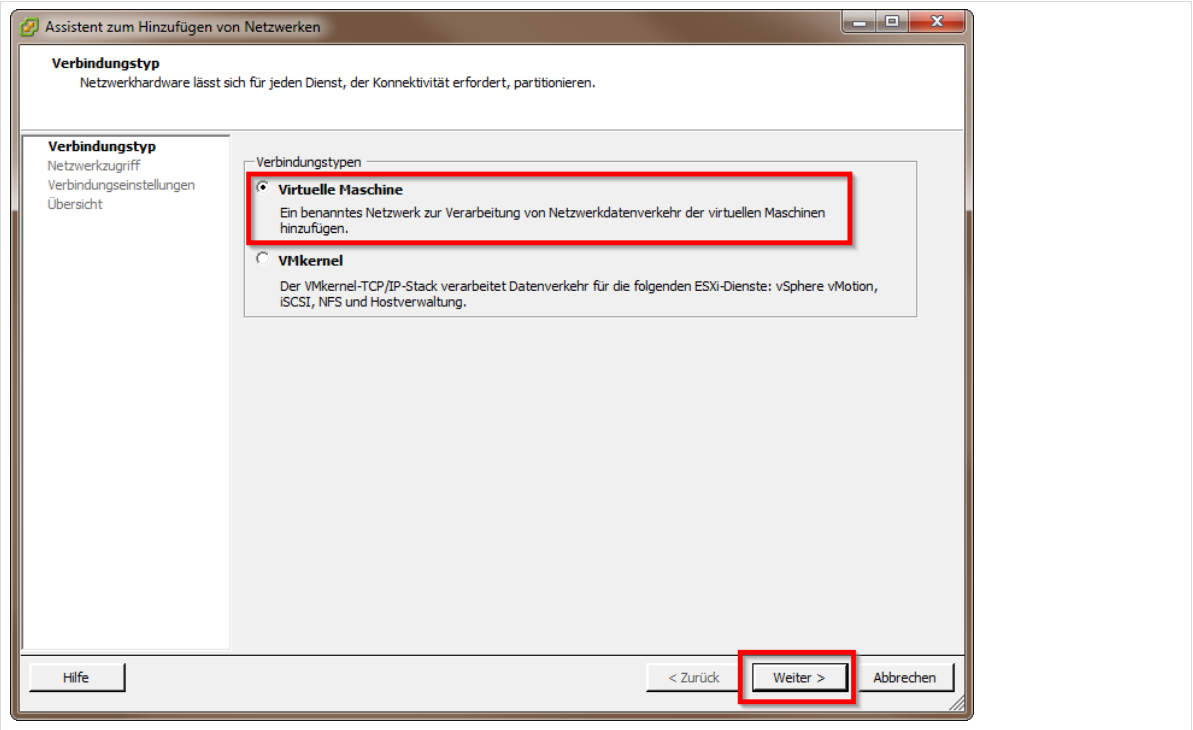


Abb. 59: Auswählen des Netzwerktyps „virtuelle Maschine“

Bestätigen Sie die Standardeinstellungen im nächsten Dialog mit Klick auf „*Weiter*“:

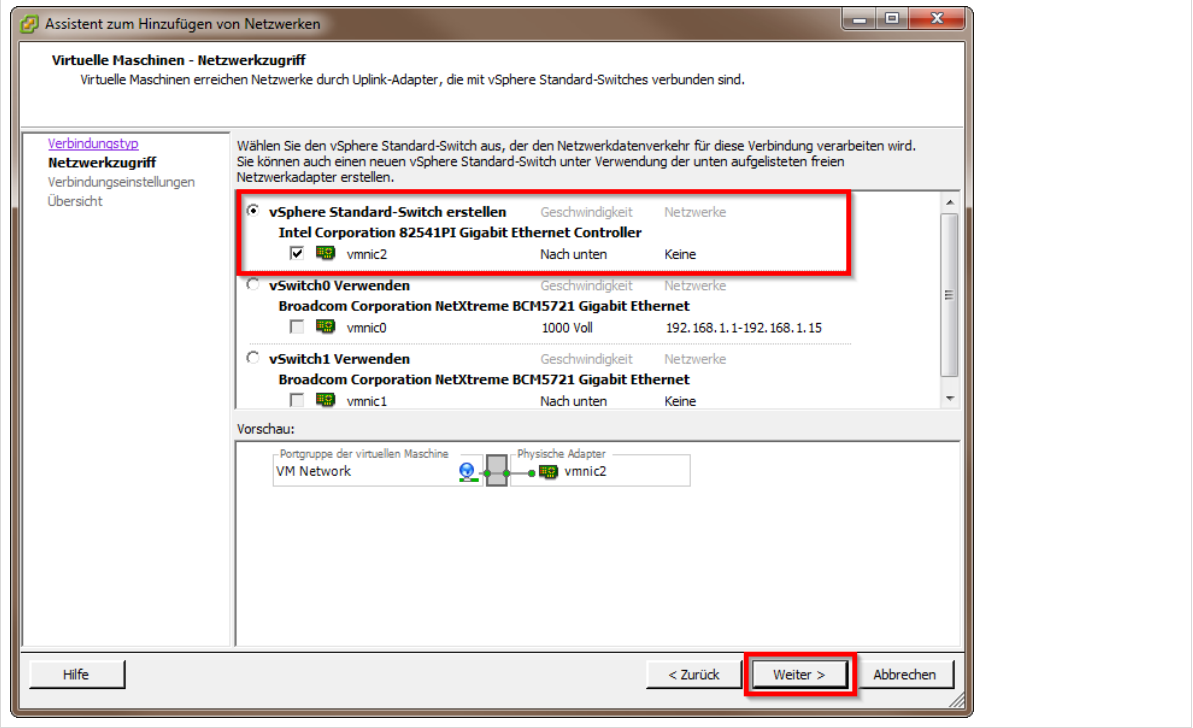


Abb. 60: Standardeinstellungen übernehmen

Geben Sie im folgenden Dialog im Feld „*Netzwerkbezeichnung*“ den Wert „*GAESTE*“ (ohne Umlaut, Großschreibung!) ein und bestätigen Sie dann mit Klick auf „*Weiter*“:

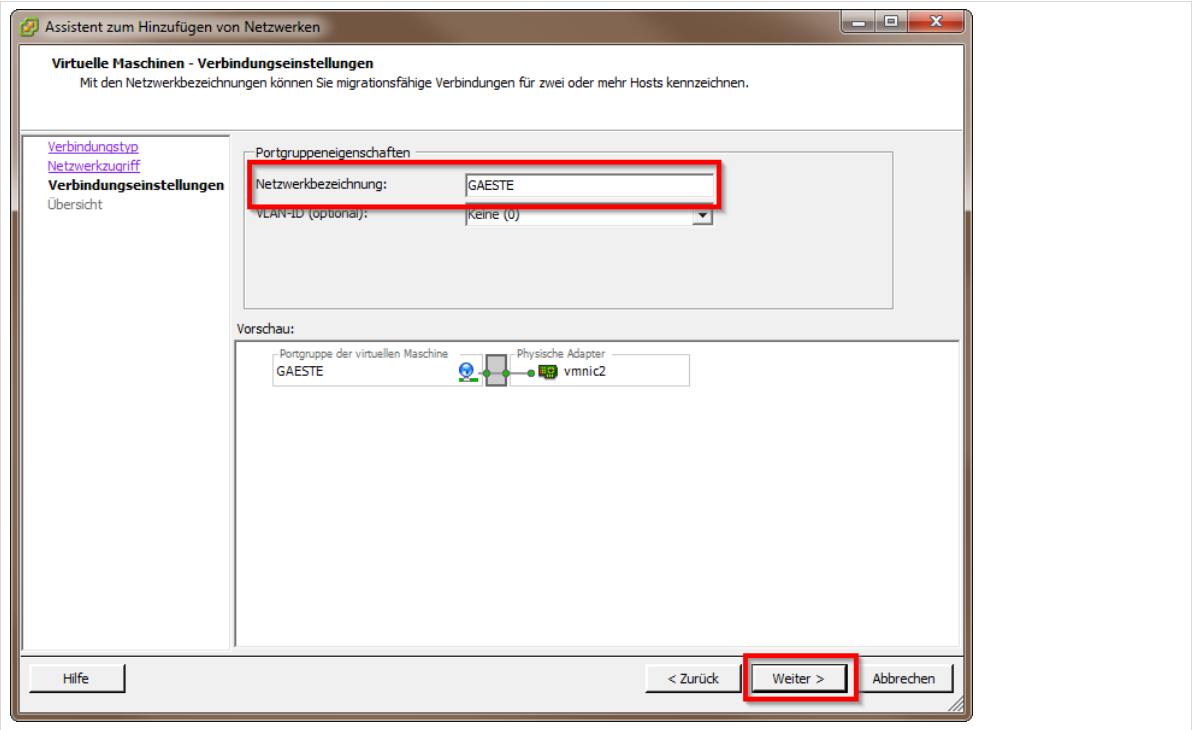


Abb. 61: Bezeichnen des neuen Netzwerks mit „GAESTE“

Bestätigen Sie den nachfolgenden Dialog mit Klick auf „*Beenden*“:

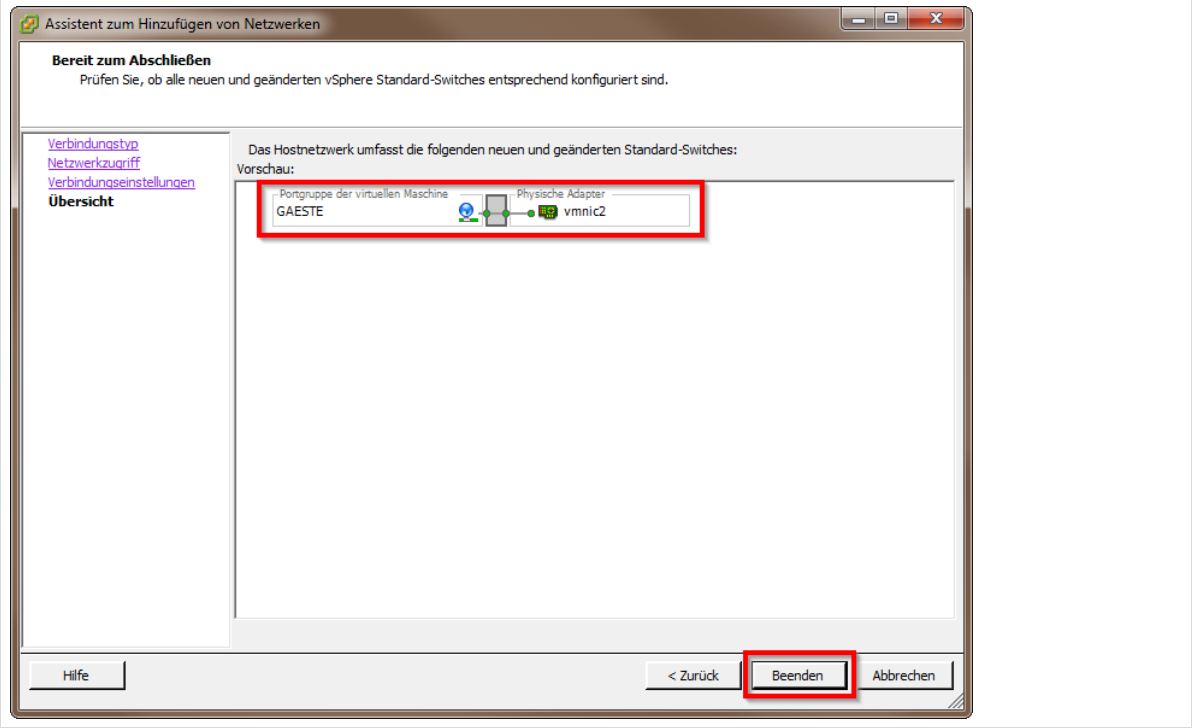


Abb. 62: Abschließen der Einrichtung des Netzwerks „GAESTE“

3.1.4 Überprüfen der virtuellen Netze

Sie sollten auf dem Virtualisierungs-Host nun die drei nachstehend abgebildeten virtuellen Netzwerke „*INTERNET*“, „*PAEDAGOGIK*“ und „*GAESTE*“ vorfinden:

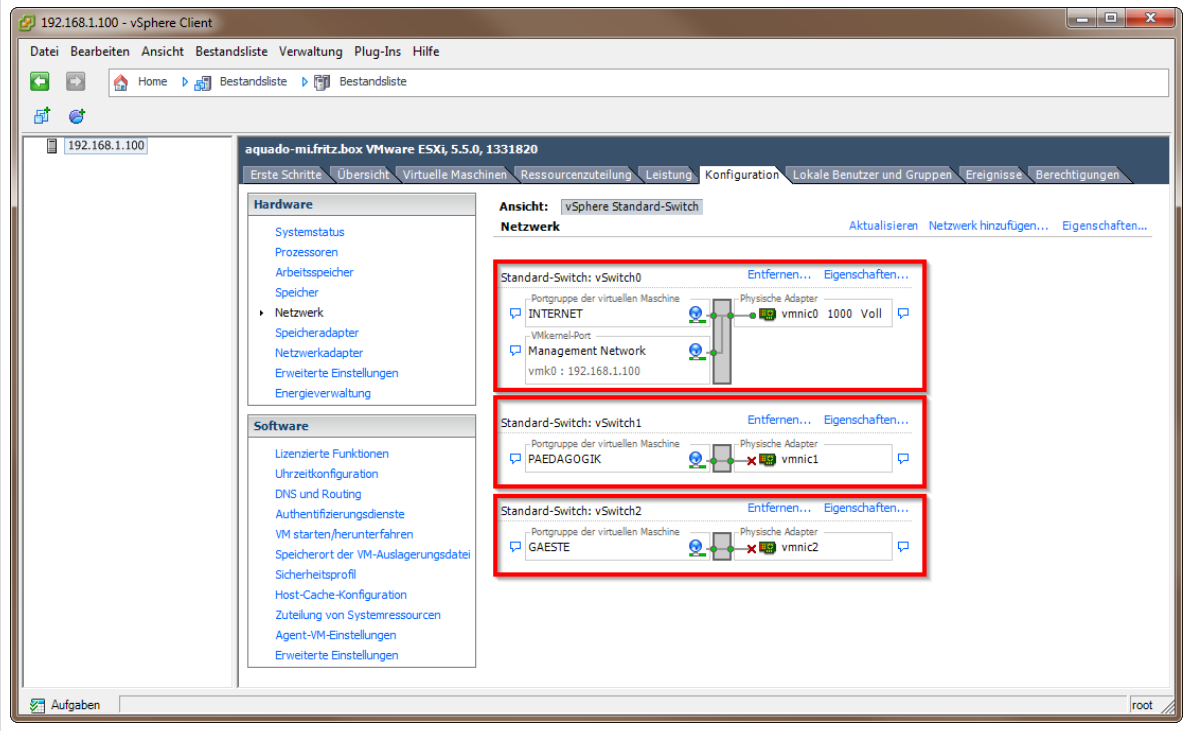


Abb. 63: Übersicht der auf dem Virtualisierungs-Host eingerichteten Netze

virtuelles Netz	Bedeutung	Physischer Adapter
„INTERNET“	Verbindung der Firewall zum Internet-Router (DSL, BelWü etc.), Zugriff auf Hypervisor („Management Network“)	vmnic0
„PAEDAGOGIK“	Verbindung zum pädagogischen Netz	vmnic1
„GAESTE“	Verbindung zum Netz für Gäste-Rechner	vmnic2

Tabelle 3: Zuordnung der virtuellen Netze zu physischen Adaptern

4. Import der virtuellen Maschinen

4.1 Anlegen von Ressourcenpools

Um die im nächsten Abschnitt zu importierenden *paedML Linux*-Server in eine Organisationseinheit zusammenfassen zu können, empfiehlt es sich, hierfür per *vSphere-Client* einen sogenannten „*Ressourcenpool*“ auf dem Virtualisierungs-Host anzulegen. Klicken Sie sich hierzu, wie nachfolgend dargestellt, durch die Menüeinträge „*Datei* | *Neu* | *Ressourcenpool*“:

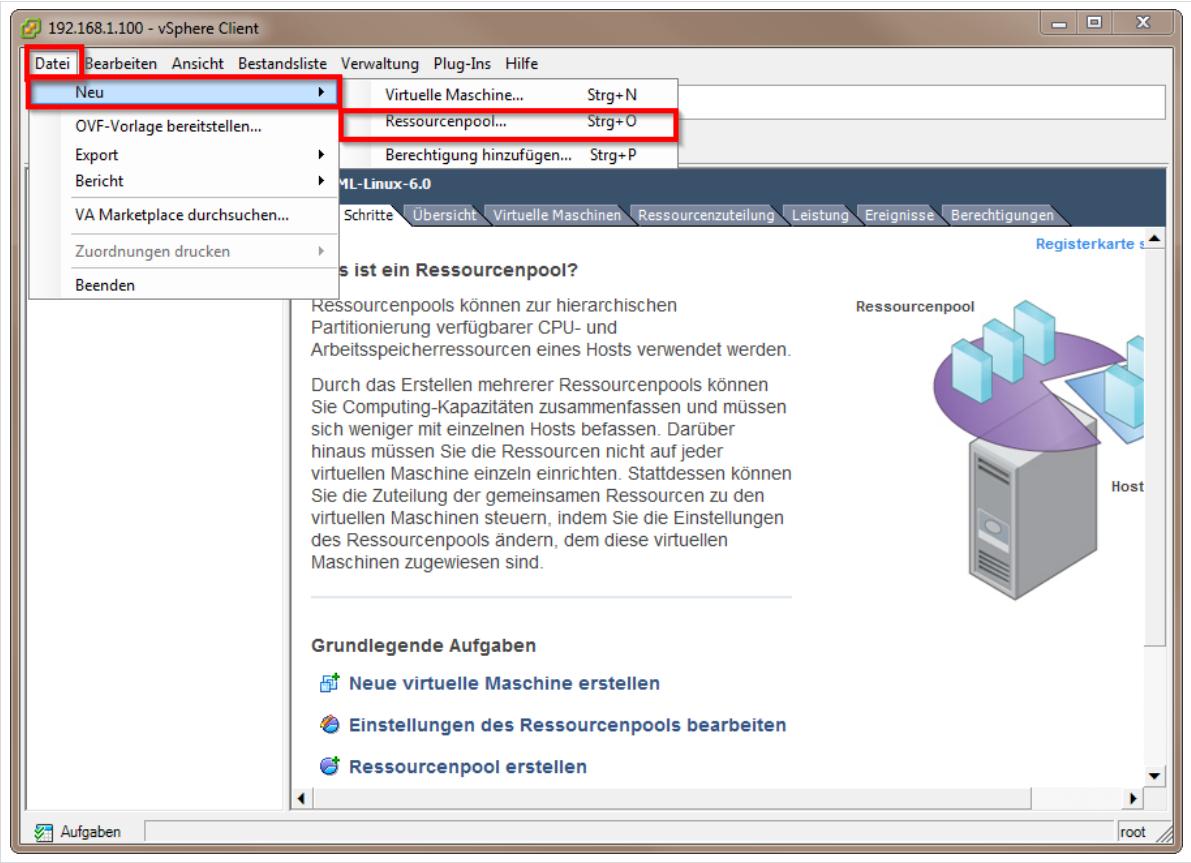


Abb. 64: Anlegen eines neuen Ressourcenpools

Tragen Sie im Feld „*Name*“ die Bezeichnung „*paedML-Linux-6.0*“ ein und bestätigen Sie mit Klick auf „*OK*“:

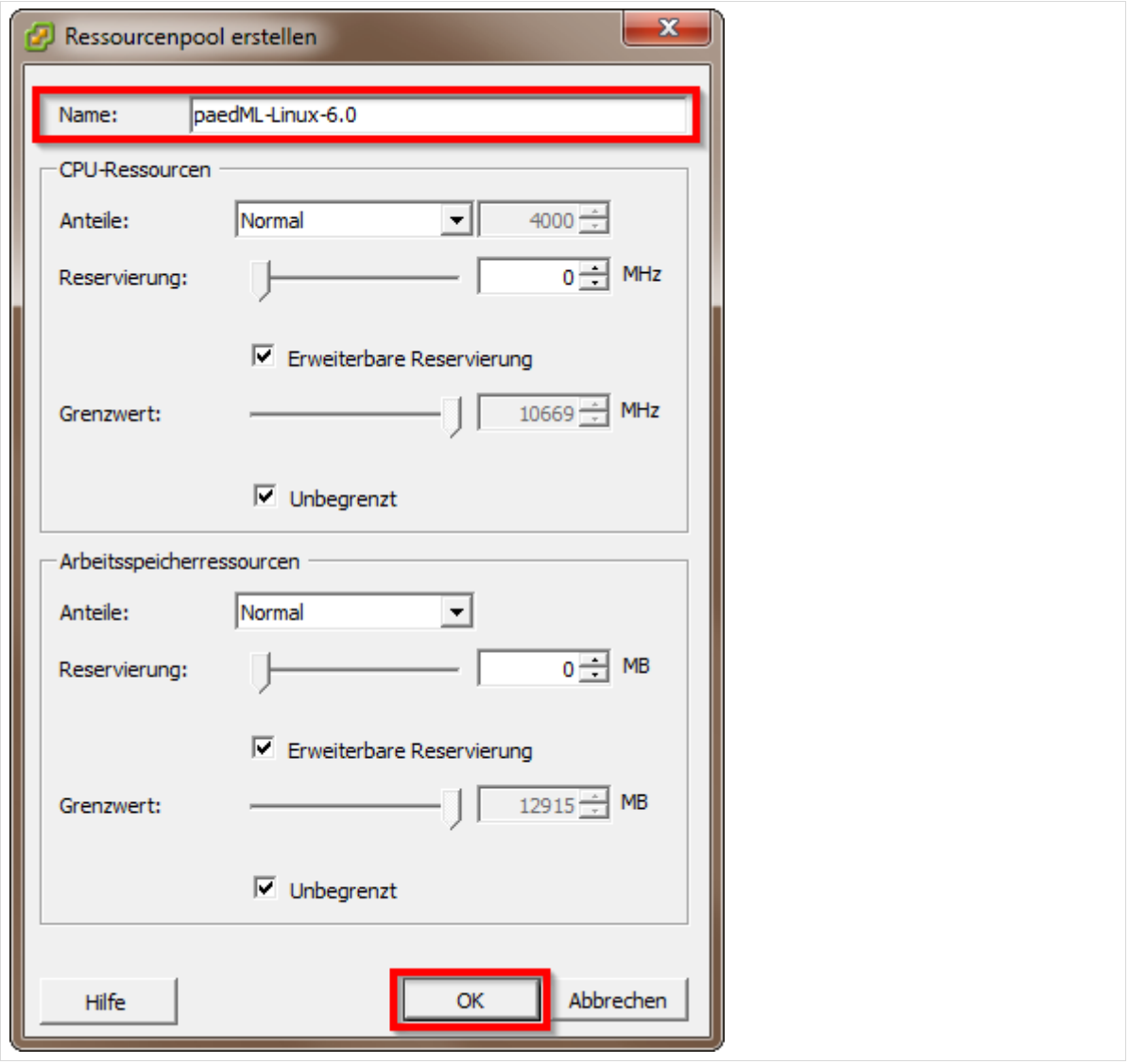


Abb. 65: Benennen des neu angelegten Ressourcenpools

Daraufhin wird der neue Ressourcenpool in der vSphere-Übersicht angezeigt:

Abb. 66: Der Ressourcenpool wurde erfolgreich angelegt.

Im Folgenden werden auf dem Virtualisierungs-Host vier virtuelle Maschinen angelegt, indem sie vom *paedML Linux*-Datenträger importiert werden.

Unterverzeichnis	Benötigte Dateien
Server	Server.mf Server.ovf Server-disk1.vmdk
opsi-Server	*opsi*-Server.mf *opsi*-Server.ovf *opsi*-Server-disk1.vmdk
Firewall	Firewall.mf Firewall.ovf Firewall-disk1.vmdk
AdminVM	AdminVM.mf AdminVM.ovf AdminVM-disk1.vmdk

Tabelle 4: Benötigte Dateien für den Import der virtuellen Maschinen

Schließen Sie zunächst den *paedML Linux*-Datenträger (USB-Stick, bestellbar über http://support-netz.de/technische-unterstuetzung/bestellen.html) an den Management-PC Ihres Virtualisierungs-Hosts an. Auf dem Datenträger sollten die in der Tabelle genannten Dateien vorhanden sein. Dabei können die drei Dateien (*.mf*, *.ovf* und *.vmdk*) auch in einer gemeinsamen Datei mit der Endung *.ova* zusammengefasst sein.

Sie können zeitgleich den Import mehrerer virtueller Maschinen ausführen.

Während zum Beispiel die virtuelle Maschine Firewall importiert wird, können Sie den Import von Server und opsi-Server ausführen.

4.2 Import der VM „Firewall“

Wählen Sie im *vSphere-Client* den zuvor erstellten Ressourcenpool per Linksklick aus:

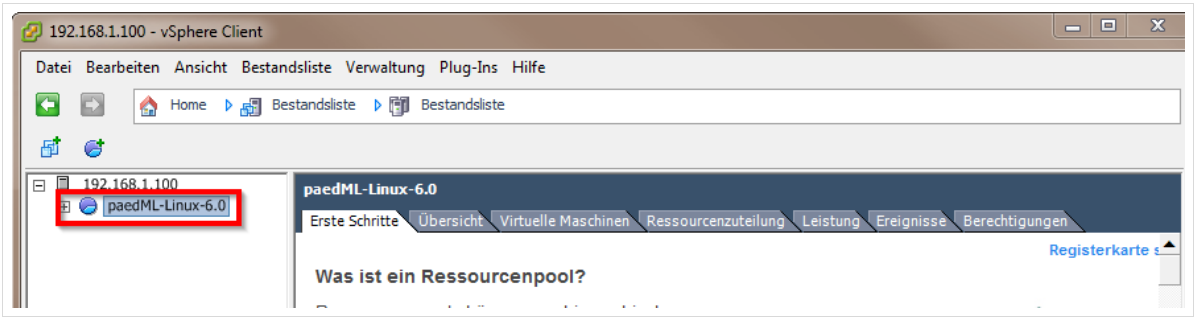


Abb. 67: Auswahl des angelegten Ressourcenpools

Wählen Sie über das Menü „*Datei*“ die Option „*OVF-Vorlage bereitstellen*“ aus:

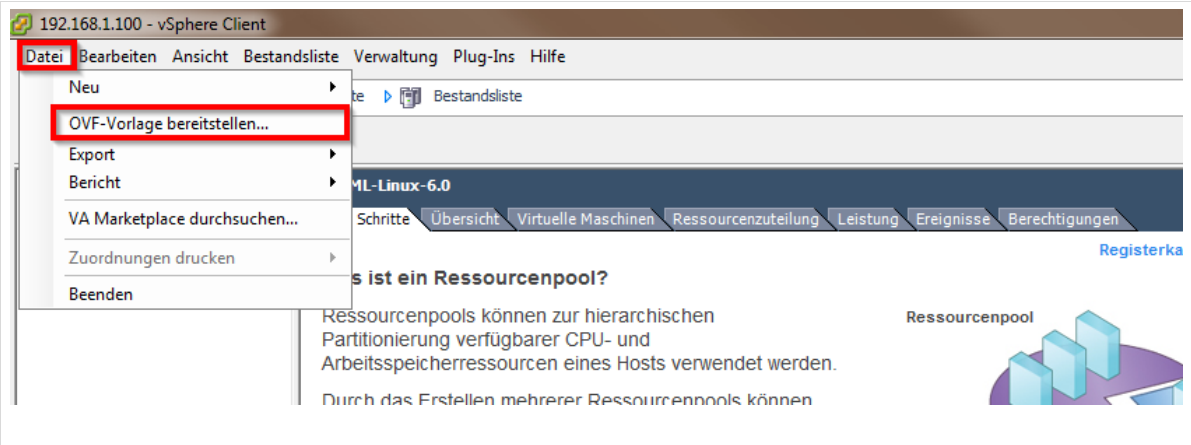


Abb. 68: Import eines OVF-Images

Klicken Sie im folgenden Assistenten auf „*Durchsuchen…*“.

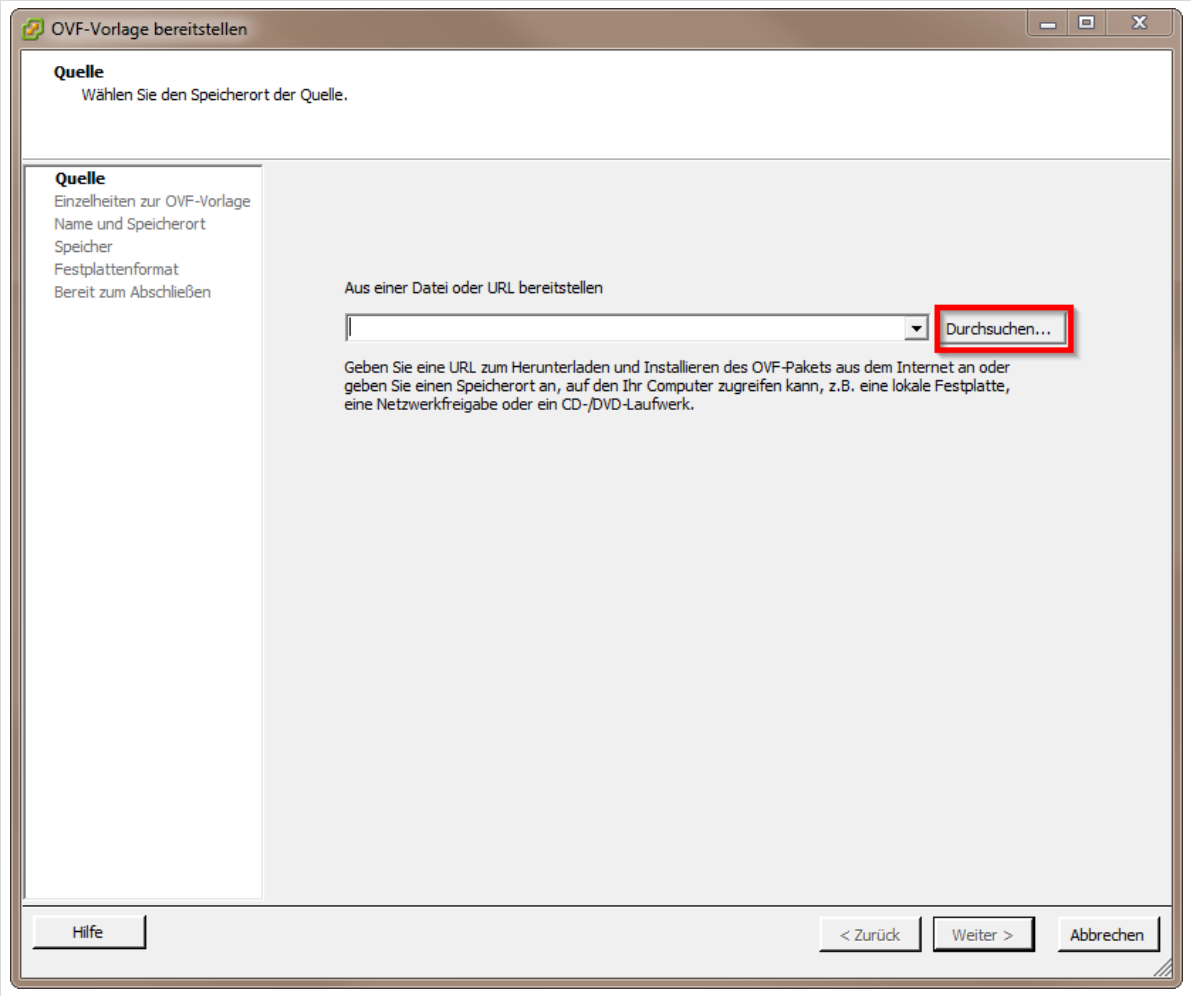

OVF-Vorlage bereitstellen
Quelle
Wählen Sie den Speicherort der Quelle.
Quelle
Einzelheiten zur OVF-Vorlage
Name und Speicherort
Speicher
Festplattenformat
Bereit zum Abschließen
Aus einer Datei oder URL bereitstellen
Durchsuchen...
Geben Sie eine URL zum Herunterladen und Installieren des OVF-Pakets aus dem Internet an oder geben Sie einen Speicherort an, auf den Ihr Computer zugreifen kann, z.B. eine lokale Festplatte, eine Netzwerkfreigabe oder ein CD-/DVD-Laufwerk.
Hilfe
< Zurück
Weiter >
Abbrechen

Abb. 69: Auswahl des zu importierenden OVF-Images für die VM „Firewall“

Wählen Sie den Pfad zum OVF-Image auf dem *paedML Linux*-Datenträger aus und klicken Sie auf „*Öffnen*“:

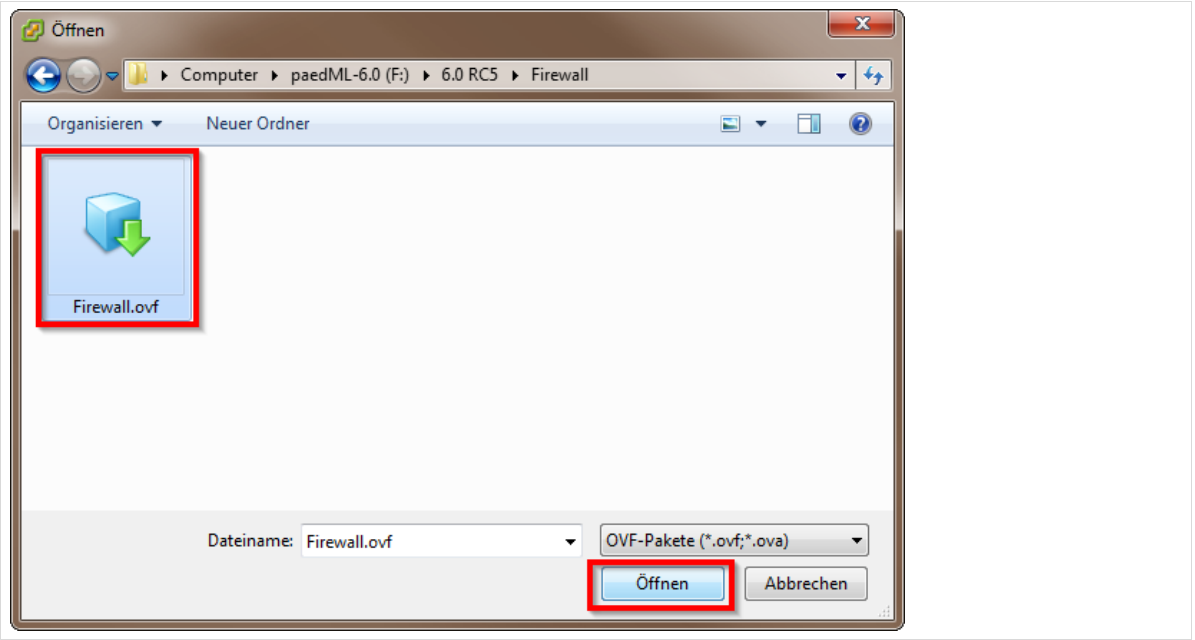


Abb. 70: Auswahl der OVF-Vorlage

Klicken Sie im nächsten Fenster auf „*Weiter*“:

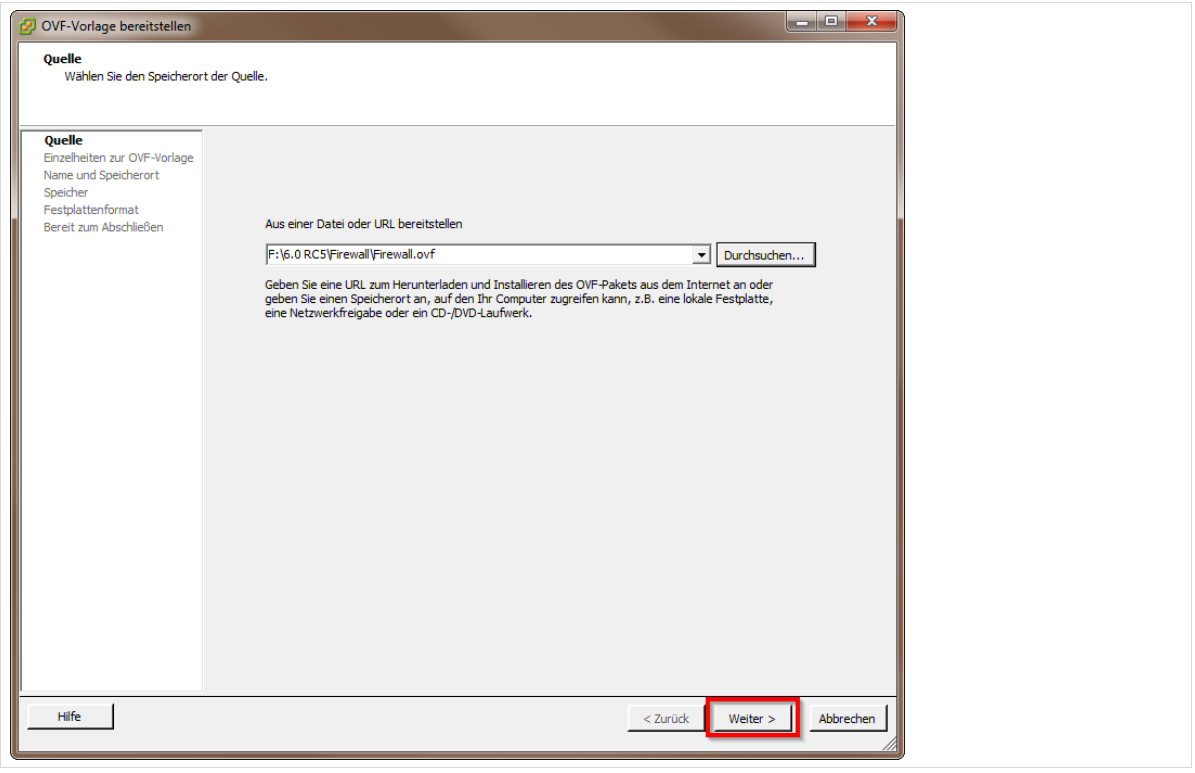

OVF-Vorlage bereitstellen
Quelle
Wählen Sie den Speicherort der Quelle.
Quelle
Einzelheiten zur OVF-Vorlage
Name und Speicherort
Speicher
Festplattenformat
Bereit zum Abschließen
Aus einer Datei oder URL bereitstellen
F:\6.0 RC5\Firewall\Firewall.ovf
Durchsuchen...
Geben Sie eine URL zum Herunterladen und Installieren des OVF-Pakets aus dem Internet an oder geben Sie einen Speicherort an, auf den Ihr Computer zugreifen kann, z.B. eine lokale Festplatte, eine Netzwerkfreigabe oder ein CD-/DVD-Laufwerk.
Hilfe
< Zurück
Weiter >
Abbrechen

Abb. 71: Der Dateipfad der OVF-Vorlage ist korrekt ausgewählt.

Im nachfolgenden Fenster werden einige Informationen zum OVF-Image angezeigt. Klicken Sie auf „*Weiter*“.

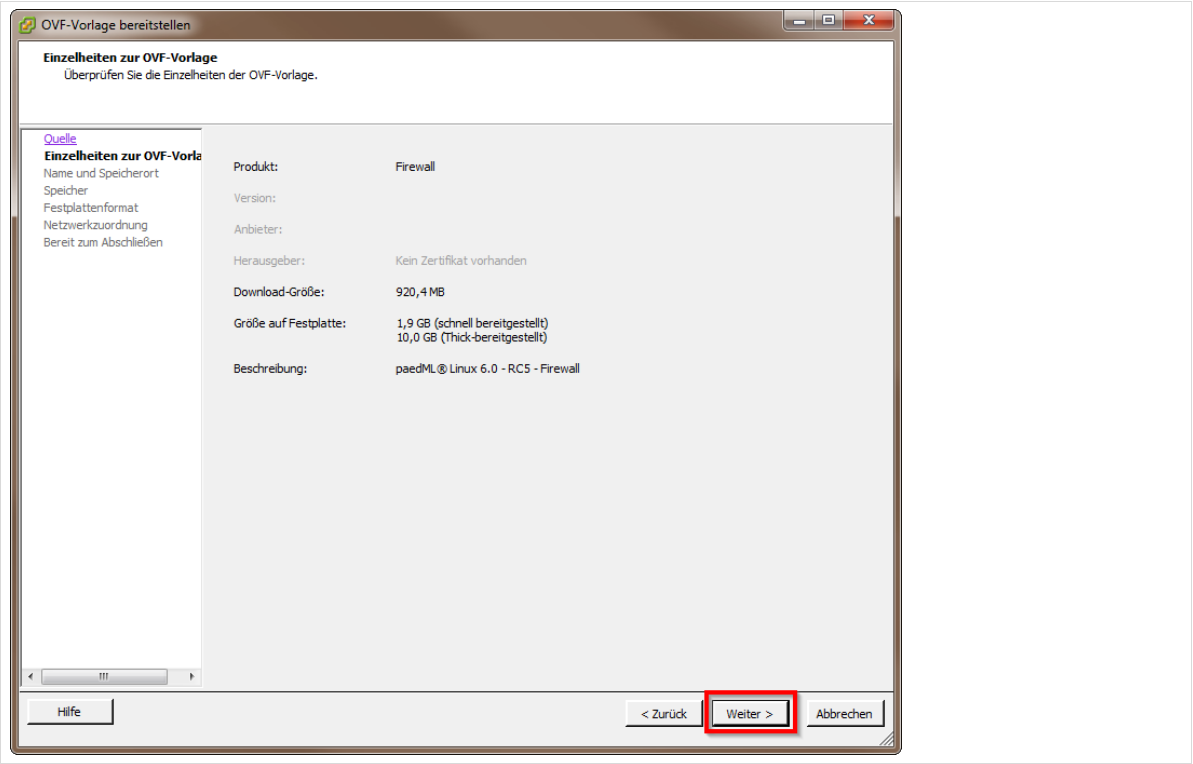


Abb. 72: Informationen zum OVF-Image

Im nächsten Fenster muss die *Endbenutzer-Lizenzvereinbarung* („*EULA*“) durch Klick auf „*Akzeptieren*“ angenommen werden.

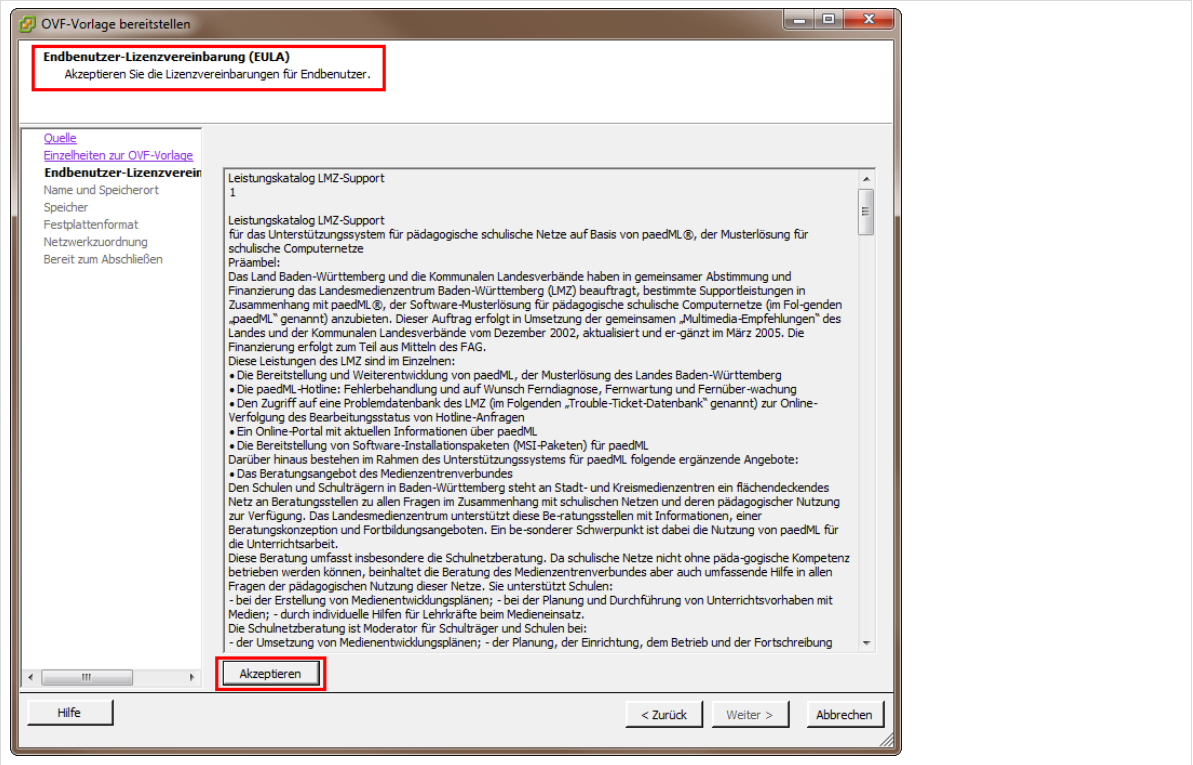

OVF-Vorlage bereitstellen
Endbenutzer-Lizenzvereinbarung (EULA)
Akzeptieren Sie die Lizenzvereinbarungen für Endbenutzer.
Quelle
Einzelheiten zur OVF-Vorlage
Endbenutzer-Lizenzverein
Name und Speicherort
Speicher
Festplattenformat
Netzwerkzuordnung
Bereit zum Abschließen
Leistungskatalog LMZ-Support
1
Leistungskatalog LMZ-Support
für das Unterstützungssystem für pädagogische schulische Netze auf Basis von paedML®, der Musterlösung für schulische Computernetze
Präambel:
Das Land Baden-Württemberg und die Kommunalen Landesverbände haben in gemeinsamer Abstimmung und Finanzierung das Landesmedienzentrum Baden-Württemberg (LMZ) beauftragt, bestimmte Supportleistungen in Zusammenhang mit paedML®, der Software-Musterlösung für pädagogische schulische Computernetze (im Fol-genden „paedML“ genannt) anzubieten. Dieser Auftrag erfolgt in Umsetzung der gemeinsamen „Multimedia-Empfehlungen“ des Landes und der Kommunalen Landesverbände vom Dezember 2002, aktualisiert und er-gänzt im März 2005. Die Finanzierung erfolgt zum Teil aus Mitteln des FAG.
Diese Leistungen des LMZ sind im Einzelnen:
• Die Bereitstellung und Weiterentwicklung von paedML, der Musterlösung des Landes Baden-Württemberg
• Die paedML-Hotline: Fehlerbehandlung und auf Wunsch Ferndiagnose, Fernwartung und Fernüber-wachung
• Den Zugriff auf eine Problemdatenbank des LMZ (im Folgenden „Trouble-Ticket-Datenbank“ genannt) zur Online-Verfolgung des Bearbeitungsstatus von Hotline-Anfragen
• Ein Online-Portal mit aktuellen Informationen über paedML
• Die Bereitstellung von Software-Installationspaketen (MSI-Paketen) für paedML
Darüber hinaus bestehen im Rahmen des Unterstützungssystems für paedML folgende ergänzende Angebote:
• Das Beratungsangebot des Medienzentrenverbundes
Den Schulen und Schulträgern in Baden-Württemberg steht an Stadt- und Kreismedienzentren ein flächendeckendes Netz an Beratungsstellen zu allen Fragen im Zusammenhang mit schulischen Netzen und deren pädagogischer Nutzung zur Verfügung. Das Landesmedienzentrum unterstützt diese Be-ratungsstellen mit Informationen, einer Beratungskonzeption und Fortbildungsangeboten. Ein be-sonderer Schwerpunkt ist dabei die Nutzung von paedML für die Unterrichtsarbeit.
Diese Beratung umfasst insbesondere die Schulnetzberatung. Da schulische Netze nicht ohne päda-gogische Kompetenz betrieben werden können, beinhaltet die Beratung des Medienzentrenverbundes aber auch umfassende Hilfe in allen Fragen der pädagogischen Nutzung dieser Netze. Sie unterstützt Schulen:
- bei der Erstellung von Medienentwicklungsplänen; - bei der Planung und Durchführung von Unterrichtsvorhaben mit Medien; - durch individuelle Hilfen für Lehrkräfte beim Medieneinsatz.
Die Schulnetzberatung ist Moderator für Schulträger und Schulen bei:
- der Umsetzung von Medienentwicklungsplänen; - der Planung, der Einrichtung, dem Betrieb und der Fortschreibung
Akzeptieren
Hilfe
< Zurück
Weiter >
Abbrechen

Abb. 73: Akzeptieren der Endbenutzer-Lizenzvereinbarungen

Klicken Sie danach auf „*Weiter*“:

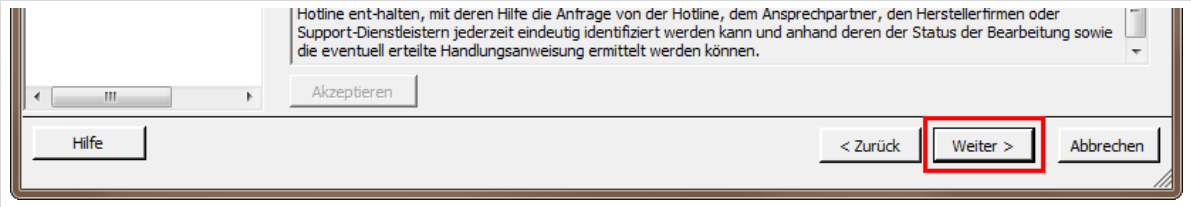

Hotline ent-halten, mit deren Hilfe die Anfrage von der Hotline, dem Ansprechpartner, den Herstellerfirmen oder Support-Dienstleistern jederzeit eindeutig identifiziert werden kann und anhand deren der Status der Bearbeitung sowie die eventuell erteilte Handlungsanweisung ermittelt werden können.
Akzeptieren
Hilfe
< Zurück
Weiter >
Abbrechen

Abb. 74: Die EULA wurde akzeptiert.

Anschließend kann ein Name für die virtuelle Maschine angegeben werden. Übernehmen Sie die Voreinstellung „*Firewall*“ und klicken Sie auf „*Weiter*“:

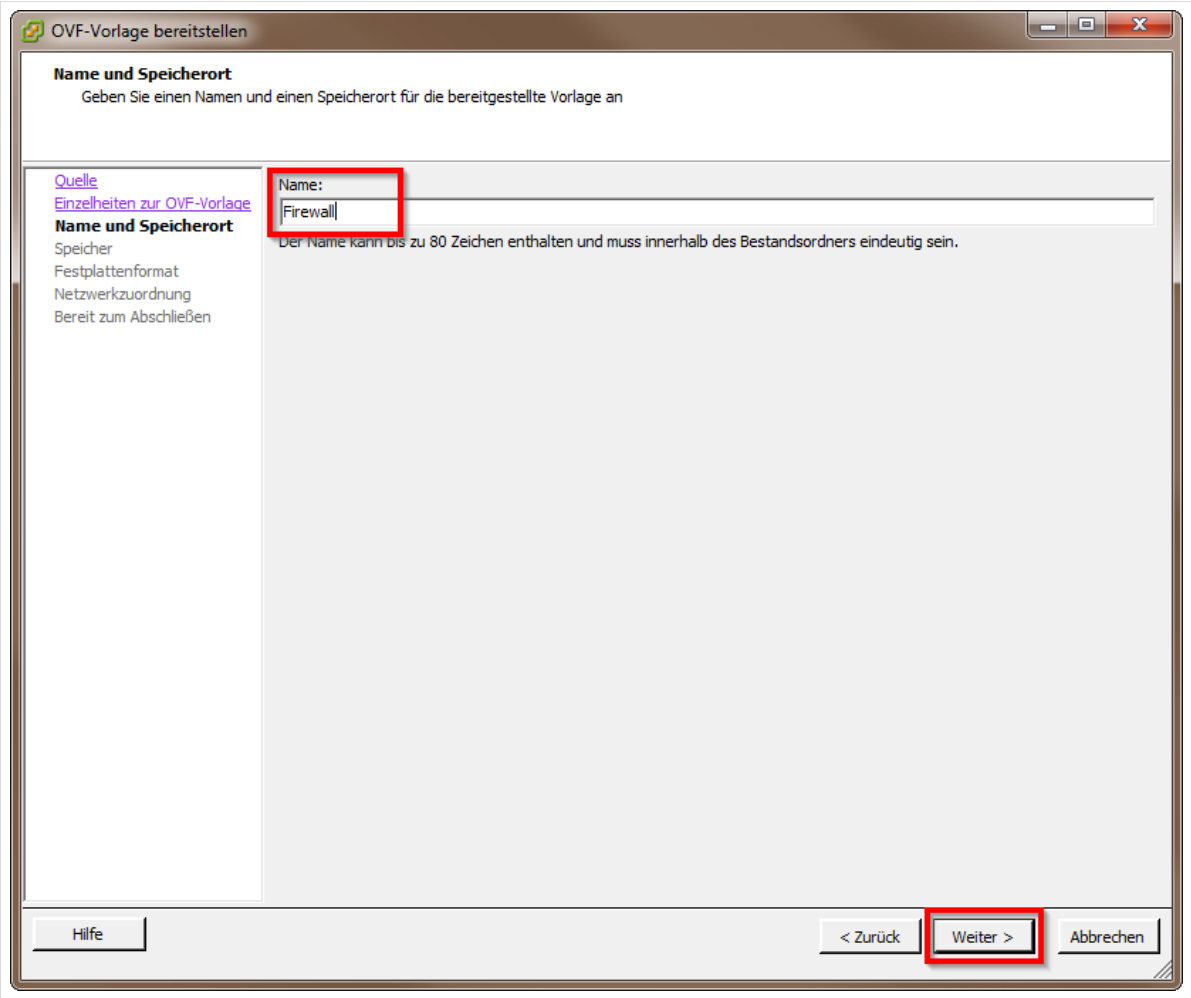


Abb. 75: Übernehmen des voreingestellten Namens „Firewall“

Sollten Sie auf dem Virtualisierungs-Host mehrere Datastores angelegt haben, müssen Sie im nächsten Dialog denjenigen Datastore auswählen, auf dem die virtuelle Maschine gespeichert werden soll. Bestätigen Sie anschließend mit „*Weiter*“.

Falls Sie nur einen einzigen Datastore angelegt haben, wird der folgende Dialog übersprungen.

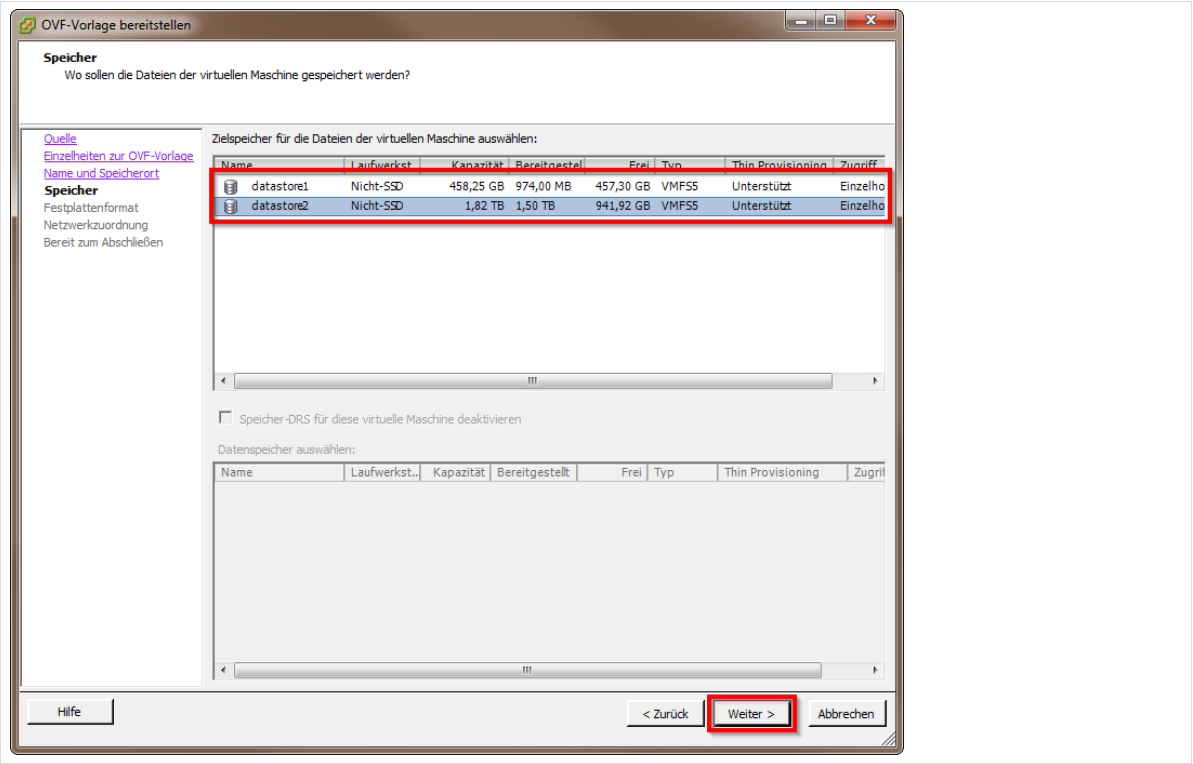


Abb. 76: Auswahl des Datastores

Im nachfolgenden Dialog wird das Festplattenformat der virtuellen Maschine festgelegt. Wählen Sie die Option „*Thick-Provision Lazy-Zeroed*“ aus und bestätigen Sie mit „*Weiter*“:

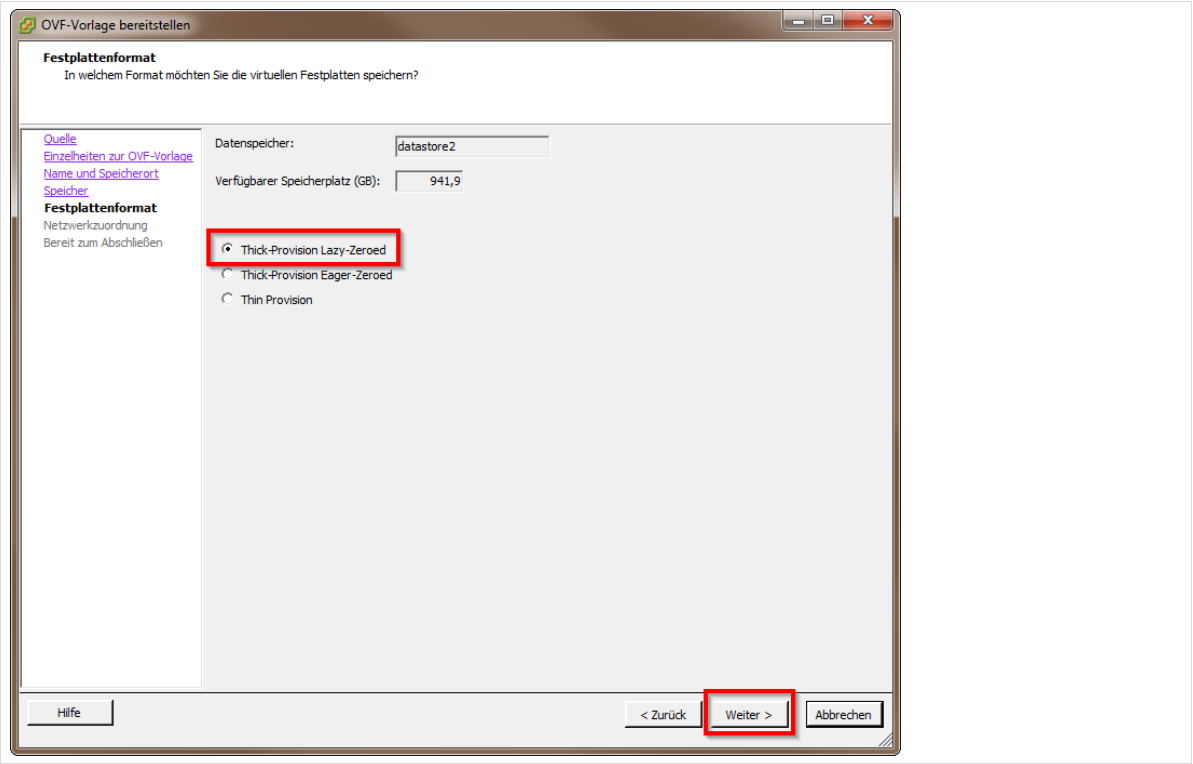


Abb. 77: Auswahl des Festplattenformats „Thick-Provision Lazy-Zeroed“

Wurden die virtuellen Netzwerke korrekt definiert und benannt, so findet die richtige Zuordnung der virtuellen Netzwerkkarten der VM „*Firewall*“, wie unten abgebildet, automatisch statt. Kontrollieren Sie die Zuordnung und korrigieren Sie diese gegebenenfalls über das Dropdownmenü. Dieses erscheint, wenn Sie auf den im Feld „*Ziellaufwerke*“ vorausgewählten Eintrag klicken. Bestätigen mit „*Weiter*“.

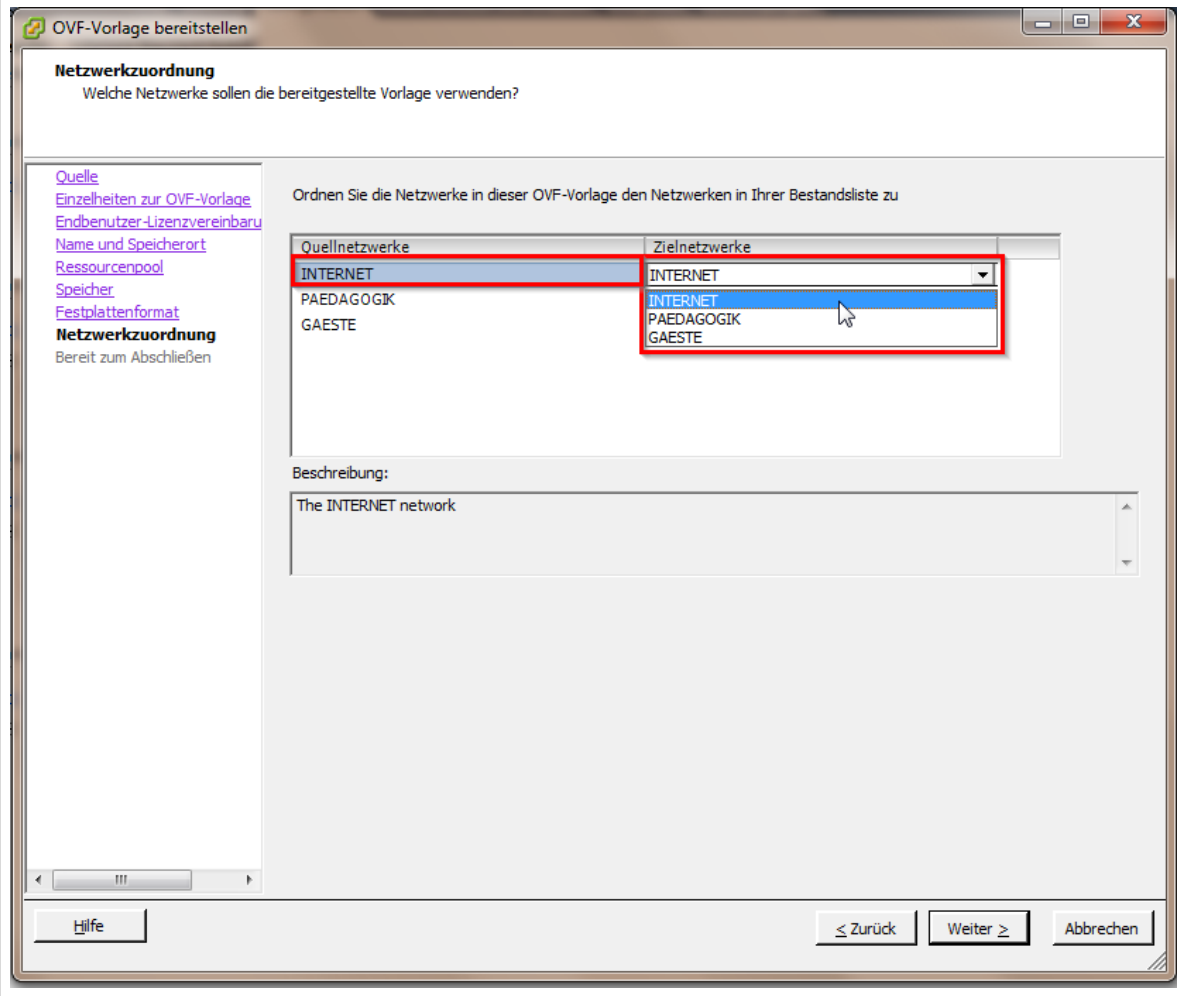


Abb. 78: Zuordnung der drei virtuellen Netzwerkkarten der Firewall zu den drei virtuellen Netzen des Virtualisierungs-Hosts

Nachfolgend werden nochmals alle Einstellungen angezeigt. Kontrollieren Sie diese Einstellungen und bestätigen Sie den Dialog mit „*Beenden*“:

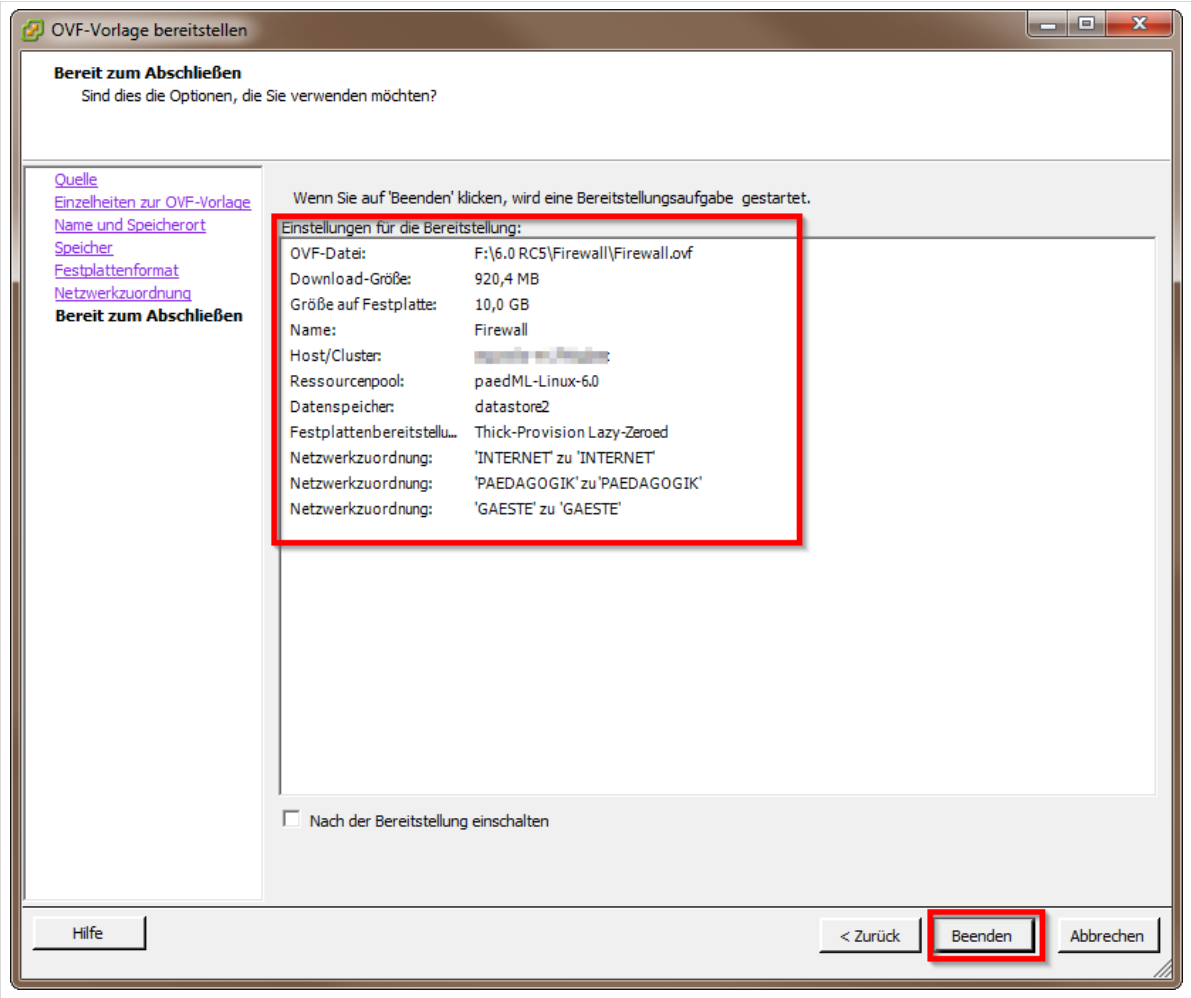


Abb. 79: Letzte Kontrolle der Einstellungen vor dem tatsächlichen Importvorgang

Nun beginnt der eigentliche Import der VM, dies kann je nach Systemleistung und Imagegröße einige Zeit in Anspruch nehmen:

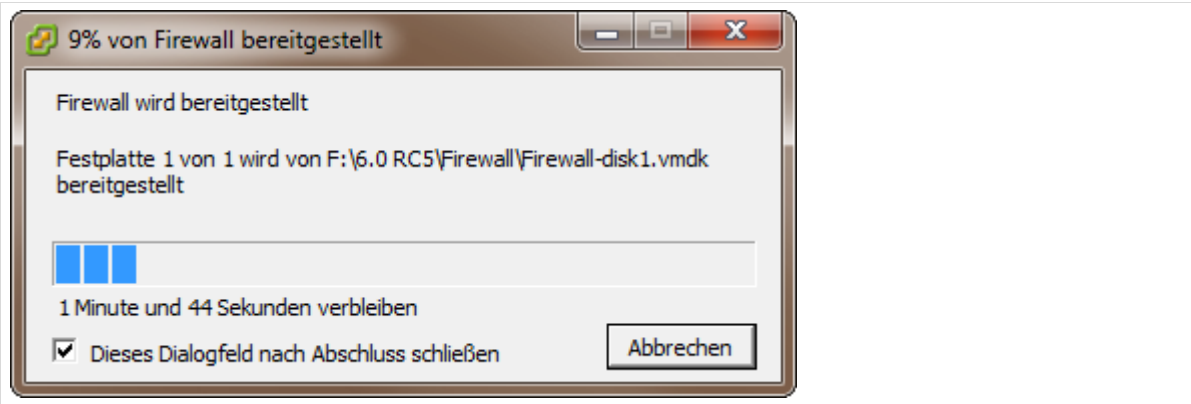

9% von Firewall bereitgestellt
Firewall wird bereitgestellt
Festplatte 1 von 1 wird von F:\6.0 RC5\Firewall\Firewall-disk1.vmdk bereitgestellt
1 Minute und 44 Sekunden verbleiben
Dieses Dialogfeld nach Abschluss schließen
Abbrechen

Abb. 80: Importvorgang der VM „Firewall“

Ein erfolgreicher Import wird wie folgt vom System quittiert, bestätigen Sie mit „*Schließen*“:

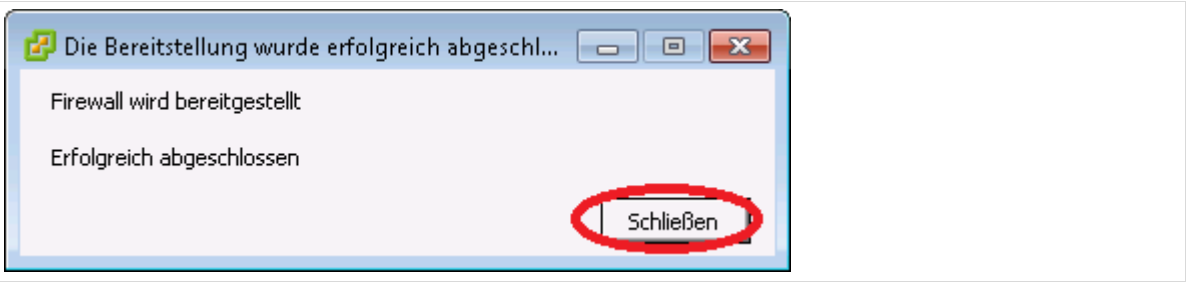


Abb. 81: Die VM „Firewall“ wurde erfolgreich importiert.

4.3 Import der VM „Server“

Wählen Sie im *vSphere-Client* den zuvor erstellten Ressourcenpool per Linksklick aus:

Abb. 82: Auswahl des Ressourcenpools

Wählen Sie über das Menü Datei die Option „*OVF-Vorlage bereitstellen*“ aus:

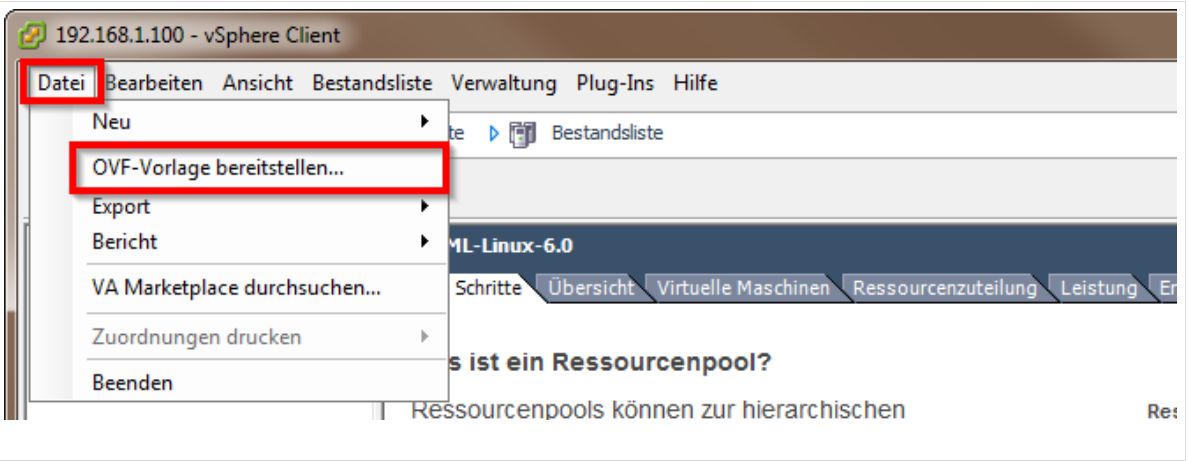


Abb. 83: OVF-Image importieren

Im nachfolgend erscheinenden Assistenten klicken Sie zunächst auf „*Durchsuchen*“:

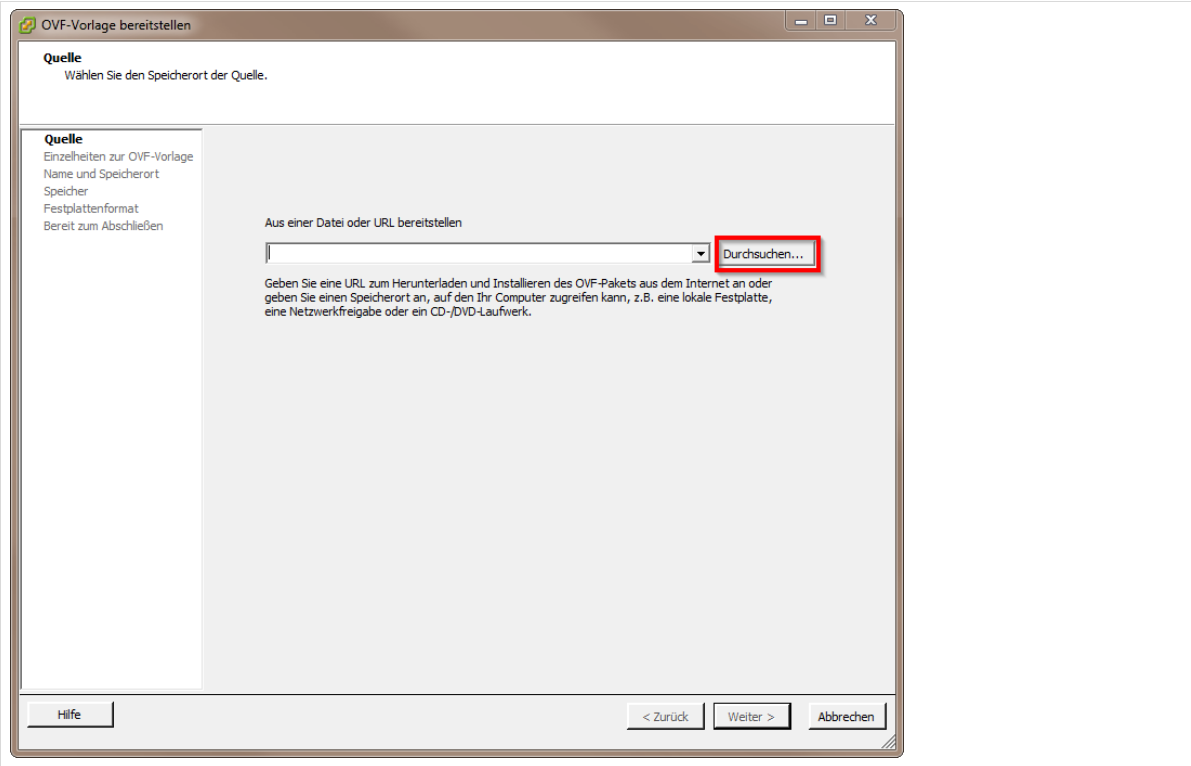

OVF-Vorlage bereitstellen
Quelle
Wählen Sie den Speicherort der Quelle.
Quelle
Einzelheiten zur OVF-Vorlage
Name und Speicherort
Speicher
Festplattenformat
Bereit zum Abschließen
Aus einer Datei oder URL bereitstellen
Durchsuchen...
Geben Sie eine URL zum Herunterladen und Installieren des OVF-Pakets aus dem Internet an oder geben Sie einen Speicherort an, auf den Ihr Computer zugreifen kann, z.B. eine lokale Festplatte, eine Netzwerkfreigabe oder ein CD-/DVD-Laufwerk.
Hilfe
< Zurück
Weiter >
Abbrechen

Abb. 84: Auswahl des zu importierenden OVF-Images für die VM „Server“

Wählen Sie den Pfad zum OVF-Image auf dem *paedML Linux*-Datenträger aus und klicken Sie auf „*Öffnen*“:

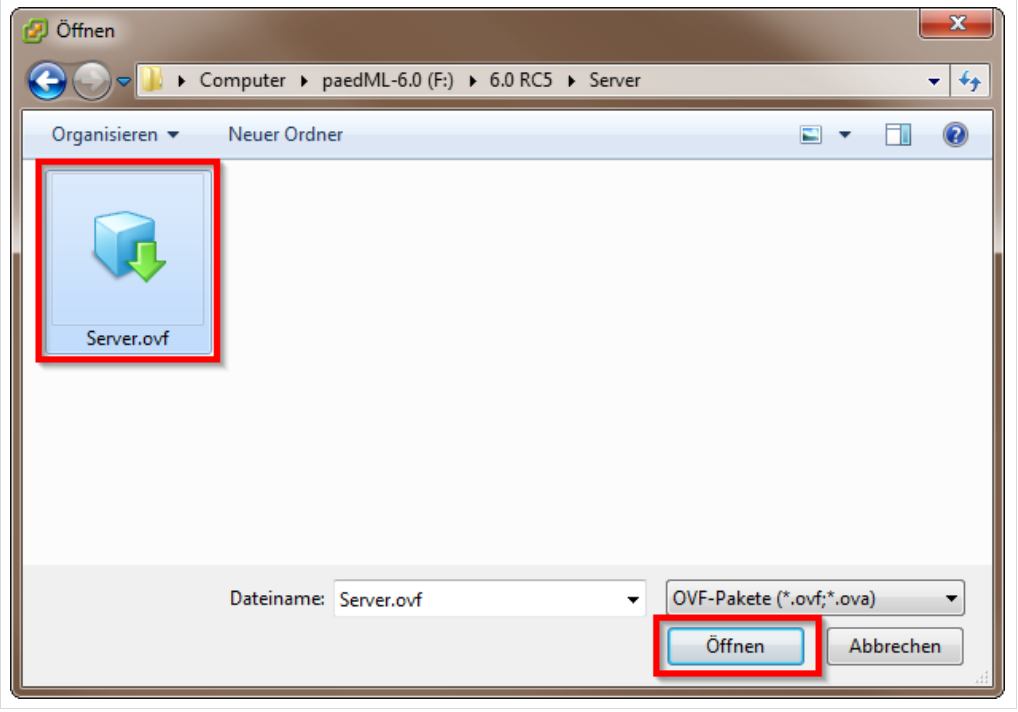


Abb. 85: Auswahl des zu importierenden OVF-Images für die VM „Server“

Bestätigen Sie im nächsten Fenster mit „*Weiter*“:

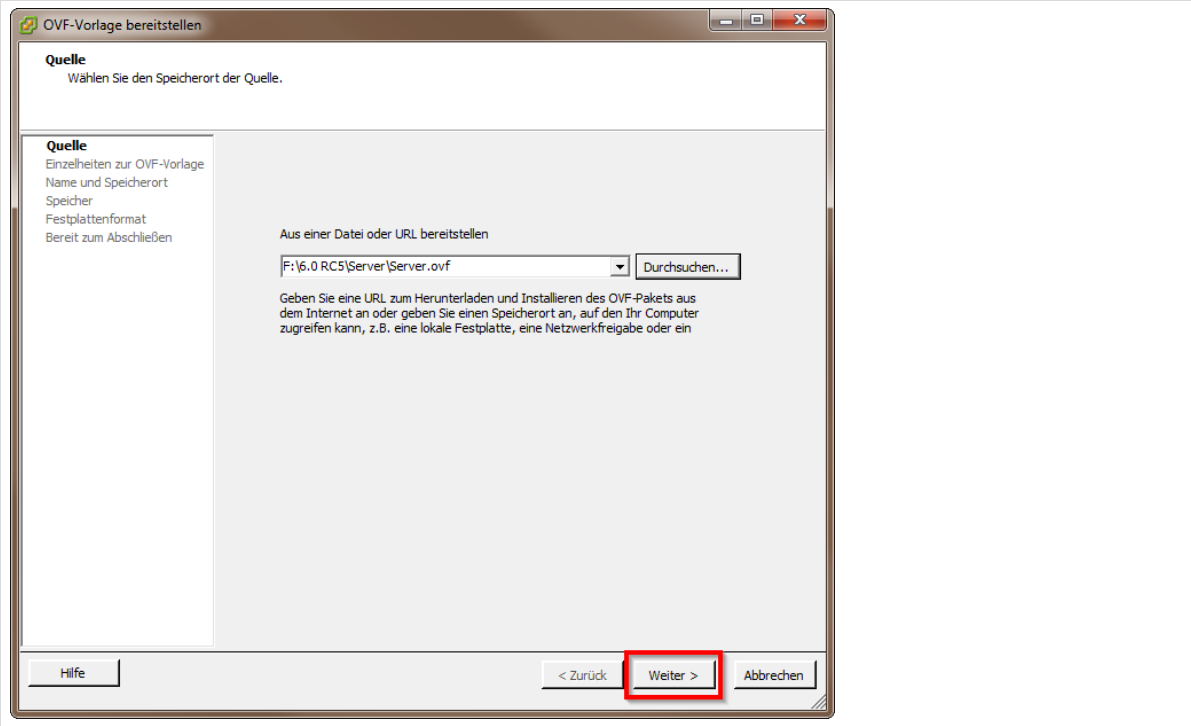

OVF-Vorlage bereitstellen
Quelle
Wählen Sie den Speicherort der Quelle.
Quelle
Einzelheiten zur OVF-Vorlage
Name und Speicherort
Speicher
Festplattenformat
Bereit zum Abschließen
Aus einer Datei oder URL bereitstellen
F:\6.0 RC5\Server\Server.ovf
Durchsuchen...
Geben Sie eine URL zum Herunterladen und Installieren des OVF-Pakets aus dem Internet an oder geben Sie einen Speicherort an, auf den Ihr Computer zugreifen kann, z.B. eine lokale Festplatte, eine Netzwerkfreigabe oder ein
Hilfe
< Zurück
Weiter >
Abbrechen

Abb. 86: Auswahl des zu importierenden OVF-Images für die VM „Server“

Im nächsten Fenster werden Informationen zum OVF-Image „*Server*“ angezeigt. Klicken Sie auf „*Weiter*“.

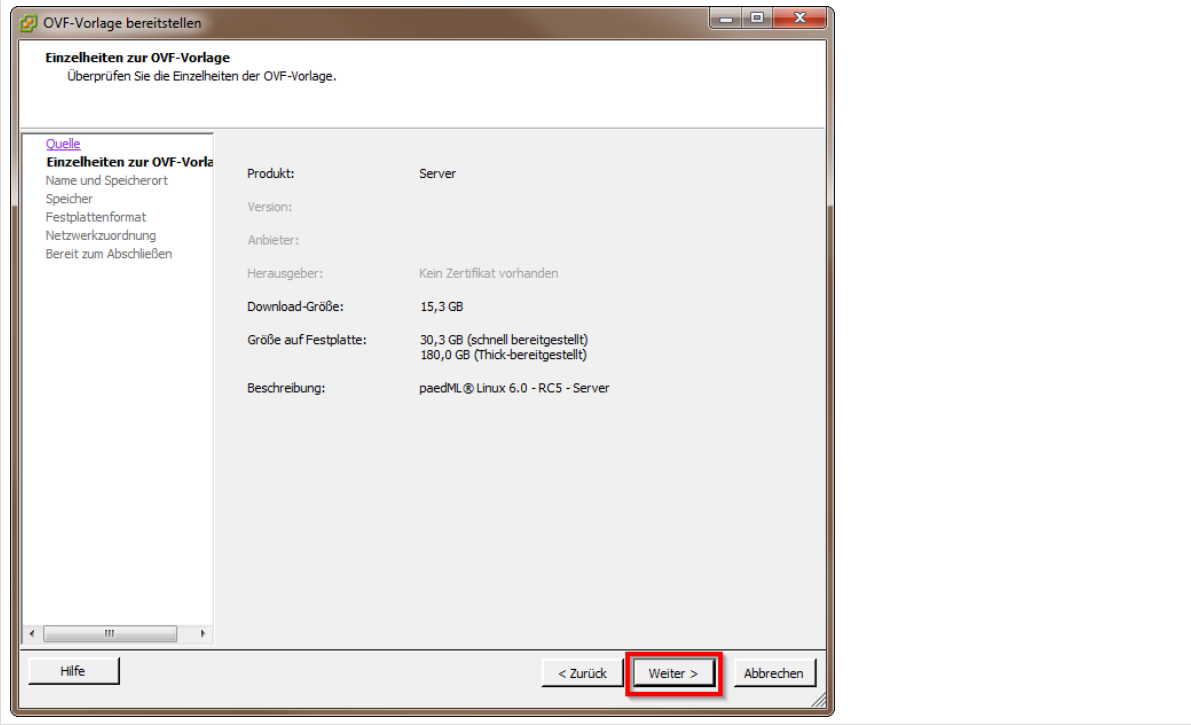


Abb. 87: Informationen zum OVF-Image „Server“

Im nächsten Fenster muss die *Endbenutzer-Lizenzvereinbarung* („*EULA*“) durch Klick auf „*Akzeptieren*“ angenommen werden.

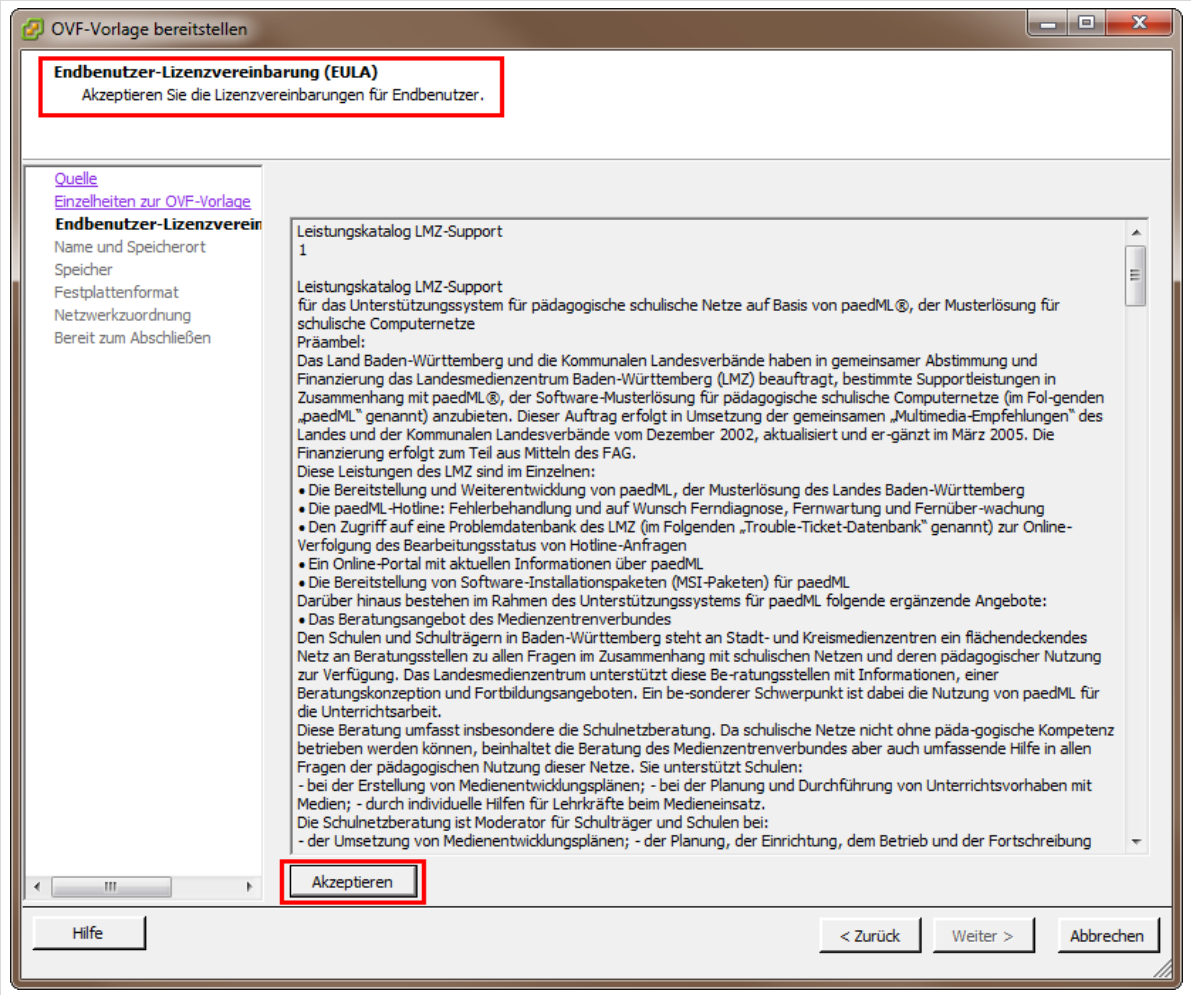

OVF-Vorlage bereitstellen
Endbenutzer-Lizenzvereinbarung (EULA)
Akzeptieren Sie die Lizenzvereinbarungen für Endbenutzer.
Quelle
Einzelheiten zur OVF-Vorlage
Endbenutzer-Lizenzverein
Name und Speicherort
Speicher
Festplattenformat
Netzwerkzuordnung
Bereit zum Abschließen
Leistungskatalog LMZ-Support
1
Leistungskatalog LMZ-Support
für das Unterstützungssystem für pädagogische schulische Netze auf Basis von paedML®, der Musterlösung für schulische Computernetze
Präambel:
Das Land Baden-Württemberg und die Kommunalen Landesverbände haben in gemeinsamer Abstimmung und Finanzierung das Landesmedienzentrum Baden-Württemberg (LMZ) beauftragt, bestimmte Supportleistungen in Zusammenhang mit paedML®, der Software-Musterlösung für pädagogische schulische Computernetze (im Fol-genden „paedML“ genannt) anzubieten. Dieser Auftrag erfolgt in Umsetzung der gemeinsamen „Multimedia-Empfehlungen“ des Landes und der Kommunalen Landesverbände vom Dezember 2002, aktualisiert und er-gänzt im März 2005. Die Finanzierung erfolgt zum Teil aus Mitteln des FAG.
Diese Leistungen des LMZ sind im Einzelnen:
• Die Bereitstellung und Weiterentwicklung von paedML, der Musterlösung des Landes Baden-Württemberg
• Die paedML-Hotline: Fehlerbehandlung und auf Wunsch Ferndiagnose, Fernwartung und Fernüber-wachung
• Den Zugriff auf eine Problemdatenbank des LMZ (im Folgenden „Trouble-Ticket-Datenbank“ genannt) zur Online-Verfolgung des Bearbeitungsstatus von Hotline-Anfragen
• Ein Online-Portal mit aktuellen Informationen über paedML
• Die Bereitstellung von Software-Installationspaketen (MSI-Paketen) für paedML
Darüber hinaus bestehen im Rahmen des Unterstützungssystems für paedML folgende ergänzende Angebote:
• Das Beratungsangebot des Medienzentrenverbundes
Den Schulen und Schulträgern in Baden-Württemberg steht an Stadt- und Kreismedienzentren ein flächendeckendes Netz an Beratungsstellen zu allen Fragen im Zusammenhang mit schulischen Netzen und deren pädagogischer Nutzung zur Verfügung. Das Landesmedienzentrum unterstützt diese Be-ratungsstellen mit Informationen, einer Beratungskonzeption und Fortbildungsangeboten. Ein be-sonderer Schwerpunkt ist dabei die Nutzung von paedML für die Unterrichtsarbeit.
Diese Beratung umfasst insbesondere die Schulnetzberatung. Da schulische Netze nicht ohne päda-gogische Kompetenz betrieben werden können, beinhaltet die Beratung des Medienzentrenverbundes aber auch umfassende Hilfe in allen Fragen der pädagogischen Nutzung dieser Netze. Sie unterstützt Schulen:
- bei der Erstellung von Medienentwicklungsplänen; - bei der Planung und Durchführung von Unterrichtsvorhaben mit Medien; - durch individuelle Hilfen für Lehrkräfte beim Medieneinsatz.
Die Schulnetzberatung ist Moderator für Schulträger und Schulen bei:
- der Umsetzung von Medienentwicklungsplänen; - der Planung, der Einrichtung, dem Betrieb und der Fortschreibung
Akzeptieren
Hilfe
< Zurück
Weiter >
Abbrechen

Abb. 88: Akzeptieren der Endbenutzer-Lizenzvereinbarungen

Klicken Sie danach auf „*Weiter*“:

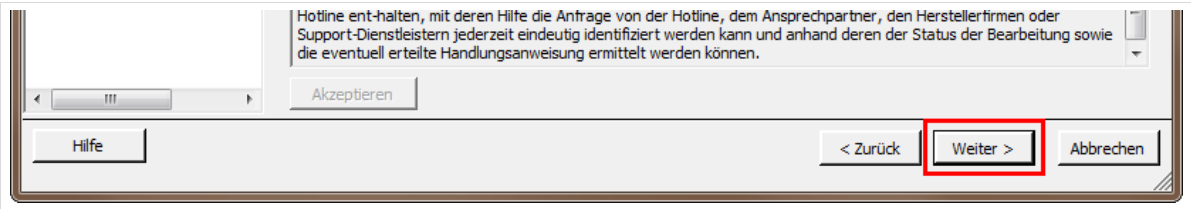

Hotline ent-halten, mit deren Hilfe die Anfrage von der Hotline, dem Ansprechpartner, den Herstellerfirmen oder Support-Dienstleistern jederzeit eindeutig identifiziert werden kann und anhand deren der Status der Bearbeitung sowie die eventuell erteilte Handlungsanweisung ermittelt werden können.
Akzeptieren
Hilfe
< Zurück
Weiter >
Abbrechen

Abb. 89: Die EULA wurde akzeptiert.

Anschließend kann ein Name für die virtuelle Maschine angegeben werden.
Übernehmen Sie die Voreinstellung „*Server*“ und klicken Sie auf „*Weiter*“

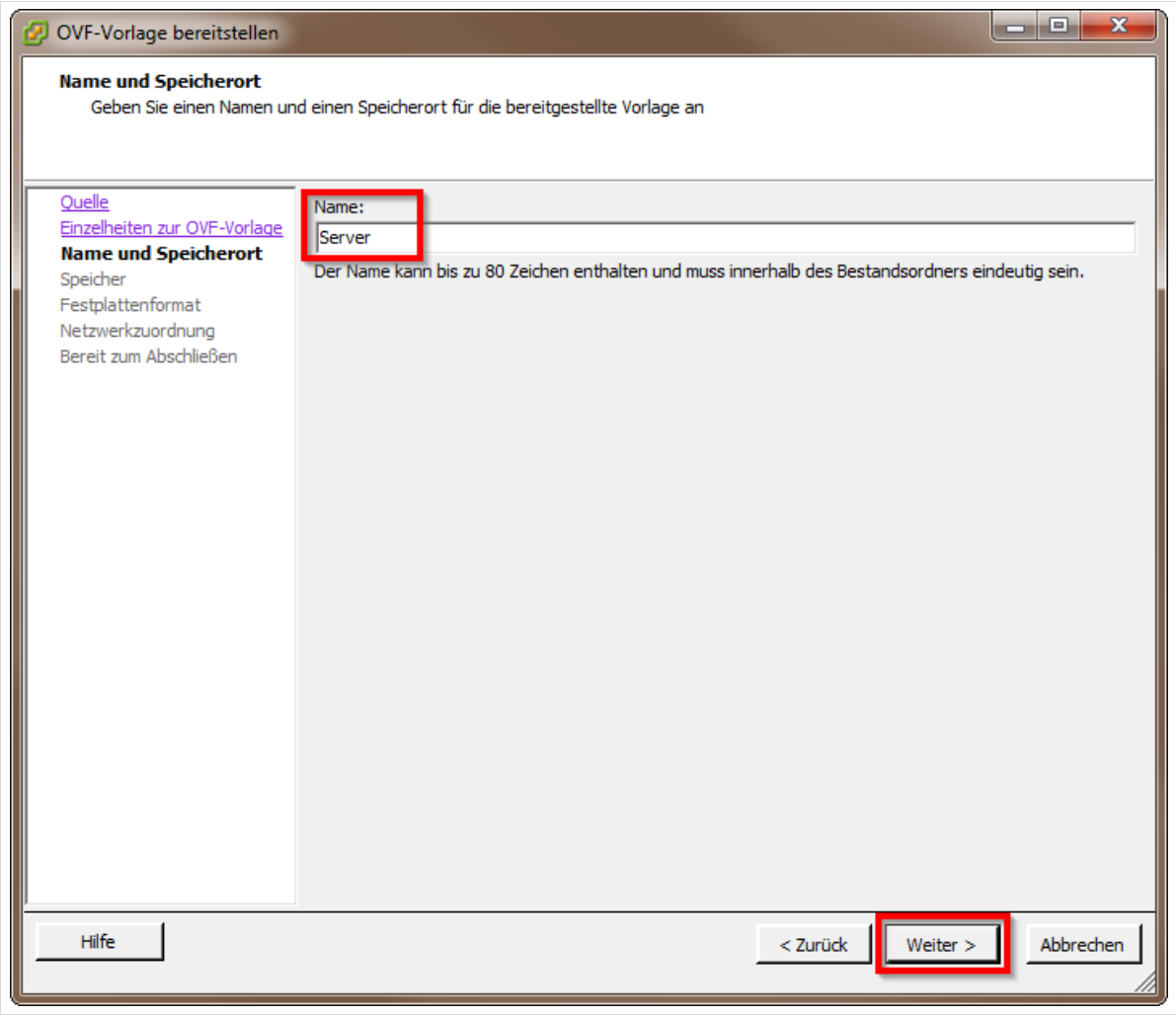


Abb. 90: Übernahme der voreingestellten Bezeichnung „Server“

Sollten Sie auf dem Virtualisierungs-Host mehrere Datastores angelegt haben, müssen Sie im nächsten Dialog denjenigen Datastore auswählen, auf dem die virtuelle Maschine gespeichert werden soll. Bestätigen Sie anschließend mit „*Weiter*“.

Falls Sie nur einen einzigen Datastore angelegt haben, wird der folgende Dialog ggf. übersprungen.

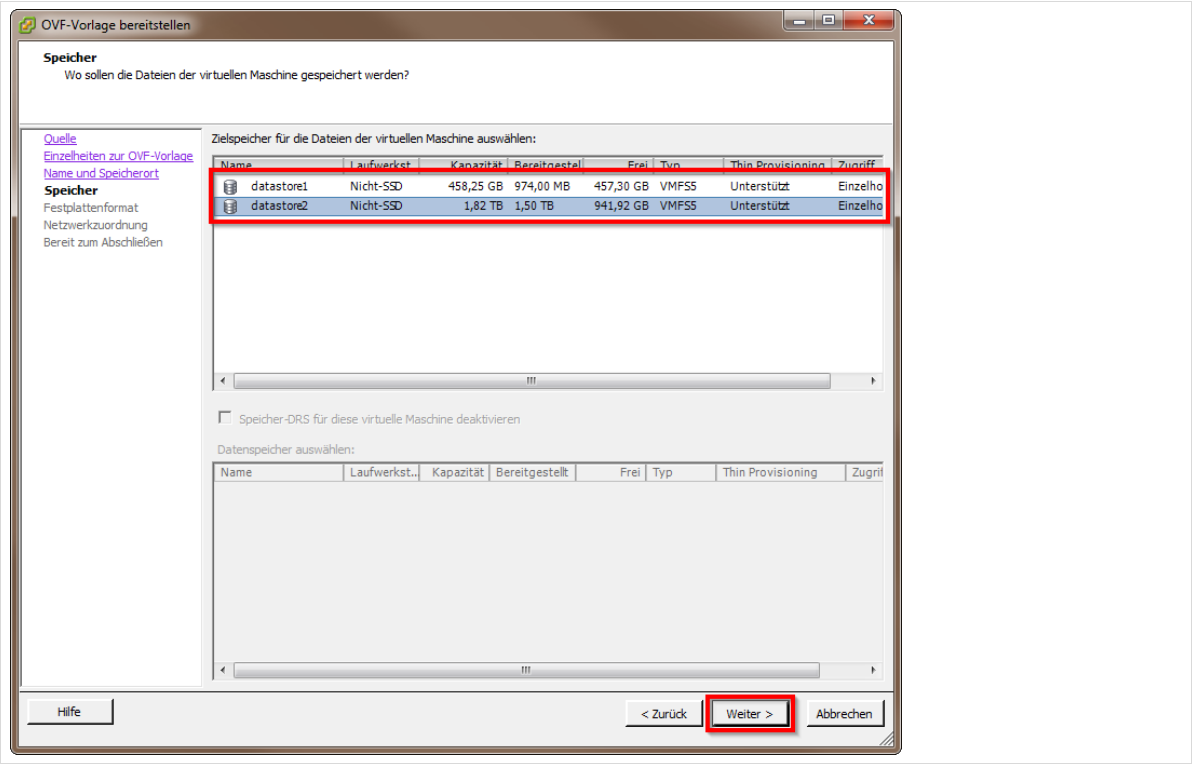


Abb. 91: Auswahl des Datastores

Im nachfolgenden Dialog wird das Festplattenformat der virtuellen Maschine festgelegt. Wählen Sie die Option „*Thick-Provision Lazy-Zeroed*“ aus und bestätigen Sie mit „*Weiter*“:

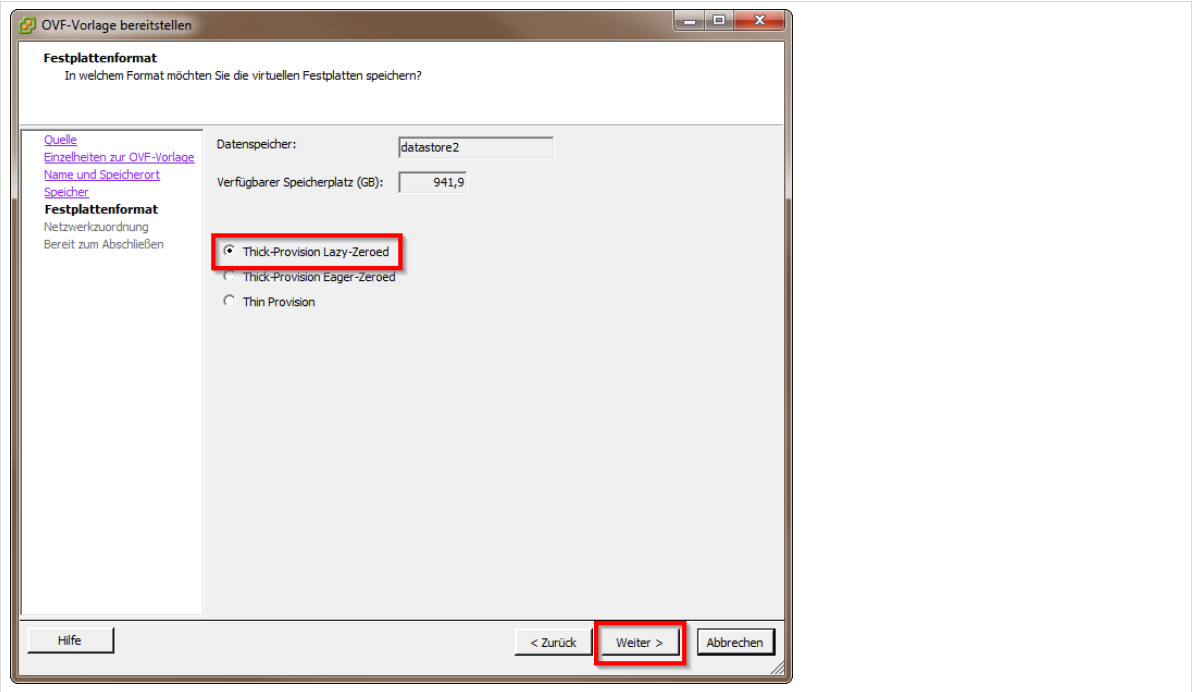


Abb. 92: Auswahl des Festplattenformats „Thick-Provision Lazy-Zeroed“

Wurden die virtuellen Netzwerke korrekt definiert, so findet die richtige Zuordnung der virtuellen Netzwerkkarte der Server-VM automatisch statt. Kontrollieren Sie die Zuordnung und korrigieren Sie diese gegebenenfalls über das Dropdownmenü. Dieses erscheint, wenn Sie auf den im Feld „*Ziellaufwerke*“ vorausgewählten Eintrag klicken. Bestätigen mit „*Weiter*“:

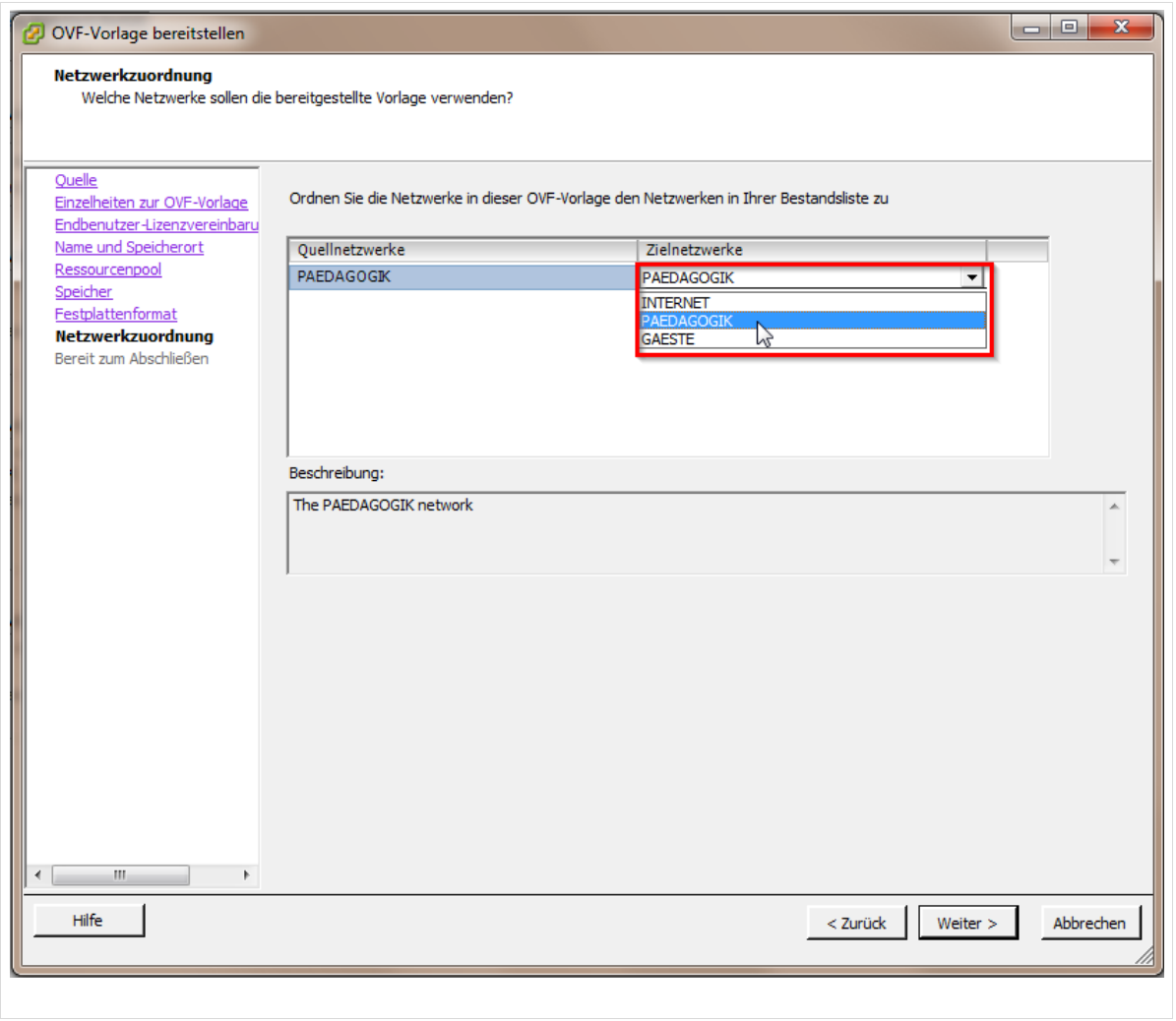


Abb. 93: Korrekte Zuordnung der virtuellen Netzwerkkarte der VM „Server“

Nachfolgend werden nochmals alle Einstellungen angezeigt. Kontrollieren Sie diese Einstellungen und bestätigen Sie den Dialog mit „*Beenden*“:

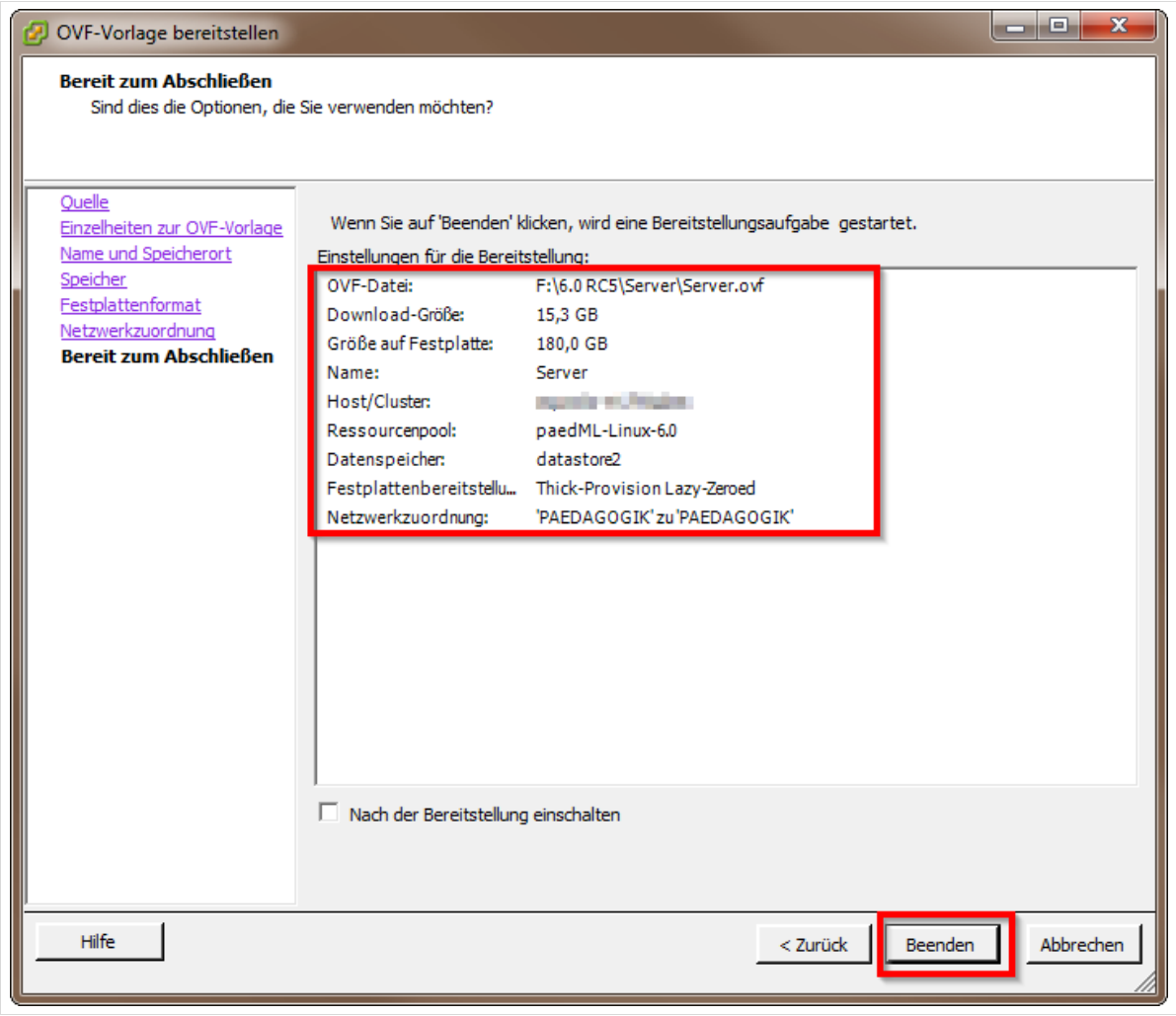


Abb. 94: Kontrolle der Einstellungen vor dem tatsächlichen Importvorgang

Nun beginnt der eigentliche Import der VM, dies kann je nach Systemleistung und Imagegröße einige Zeit in Anspruch nehmen:

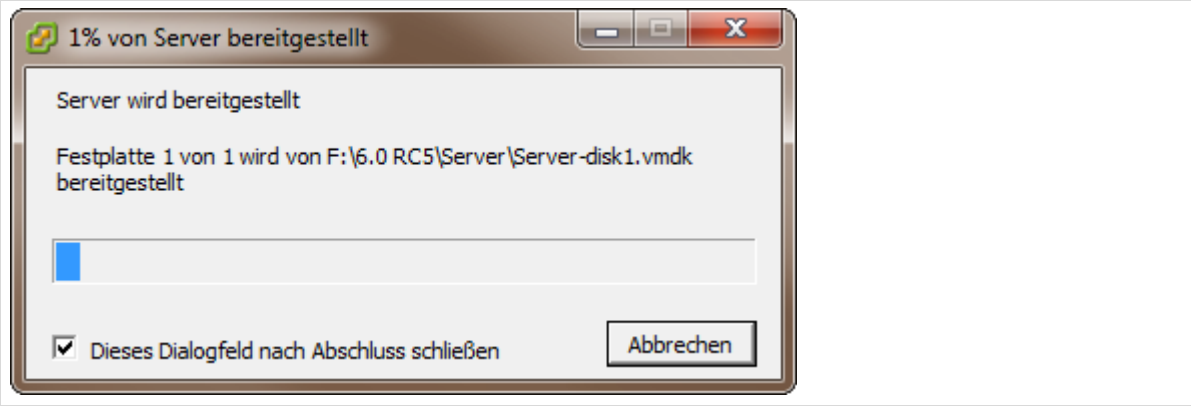

1% von Server bereitgestellt
Server wird bereitgestellt
Festplatte 1 von 1 wird von F:\6.0 RC5\Server\Server-disk1.vmdk bereitgestellt
Dieses Dialogfeld nach Abschluss schließen
Abbrechen

Abb. 95: Importvorgang der VM "Server"

Ein erfolgreicher Import wird wie folgt vom System quittiert, bestätigen Sie mit „*Schließen*“:

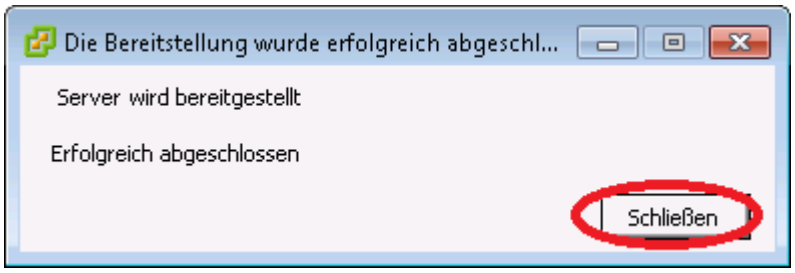


Abb. 96: Die VM „Server“ wurde erfolgreich importiert.

4.4 Import der VM „opsi-Server“

Wählen Sie im *vSphere-Client* den zuvor erstellten Ressourcenpool per Linksklick aus:

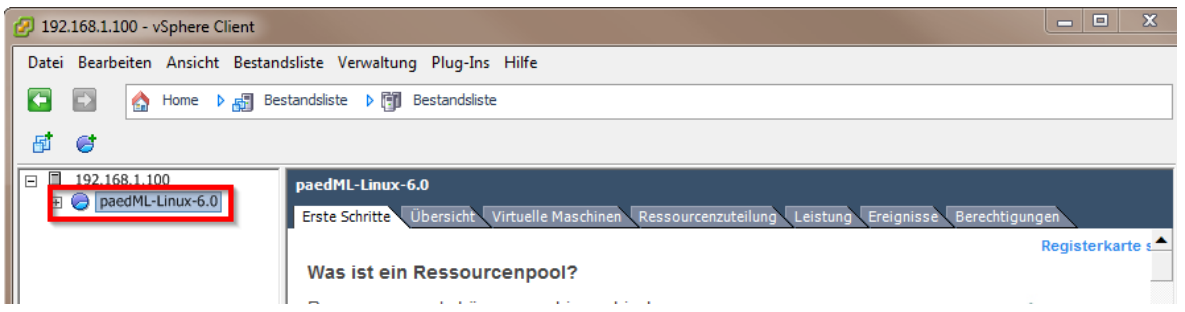


Abb. 97: Auswahl des Ressourcenpools

Wählen Sie über das Menü „*Datei*“ die Option „*OVF-Vorlage bereitstellen*“ aus:

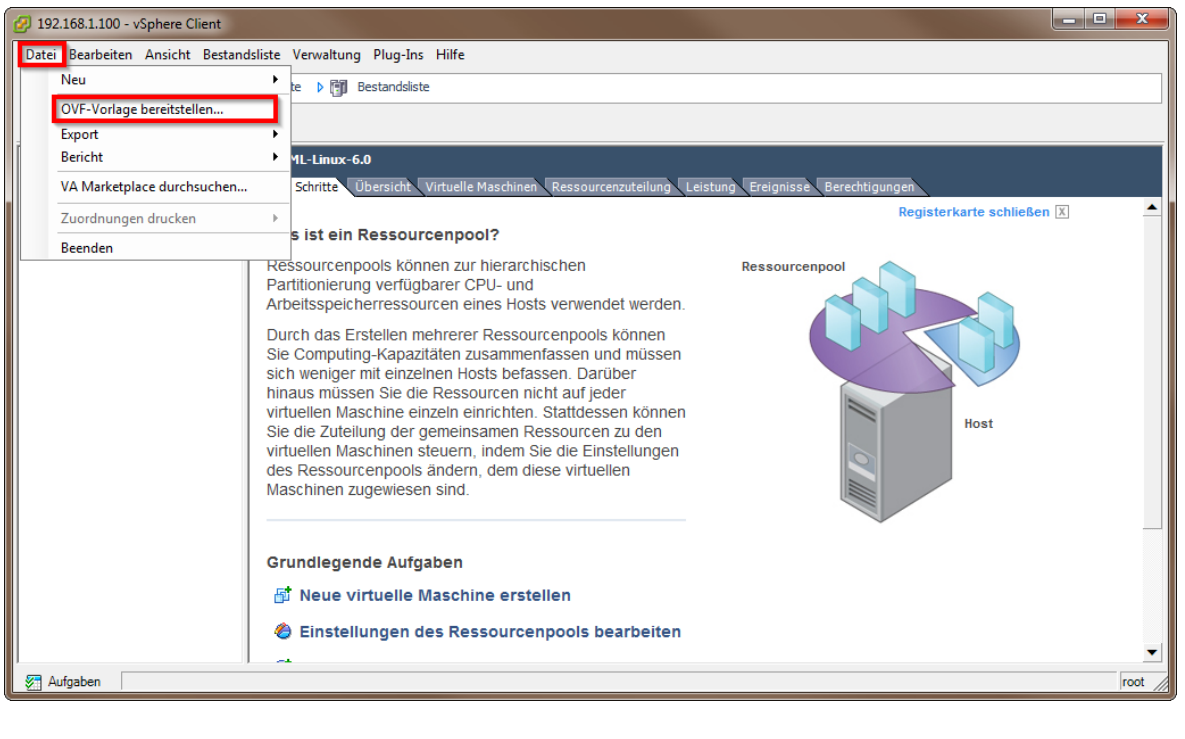

192.168.1.100 - vSphere Client
Datei Bearbeiten Ansicht Bestandsliste Verwaltung Plug-Ins Hilfe
Neu
OVF-Vorlage bereitstellen...
Export
Bericht
VA Marketplace durchsuchen...
Zuordnungen drucken
Beenden
Bestandsliste
Übersicht Virtuelle Maschinen Ressourcenzuteilung Leistung Ereignisse Berechtigungen
Registerkarte schließen
Ressourcenpool
Host
Ressourcenpools können zur hierarchischen Partitionierung verfügbarer CPU- und Arbeitsspeicherressourcen eines Hosts verwendet werden.
Durch das Erstellen mehrerer Ressourcenpools können Sie Computing-Kapazitäten zusammenfassen und müssen sich weniger mit einzelnen Hosts befassen. Darüber hinaus müssen Sie die Ressourcen nicht auf jeder virtuellen Maschine einzeln einrichten. Stattdessen können Sie die Zuteilung der gemeinsamen Ressourcen zu den virtuellen Maschinen steuern, indem Sie die Einstellungen des Ressourcenpools ändern, dem diese virtuellen Maschinen zugewiesen sind.
Grundlegende Aufgaben
Neue virtuelle Maschine erstellen
Einstellungen des Ressourcenpools bearbeiten
Aufgaben
root

Abb. 98: Import des OVF-Images „opsi-Server“

Im nachfolgend erscheinenden Assistenten klicken Sie zunächst auf „*Durchsuchen*“:

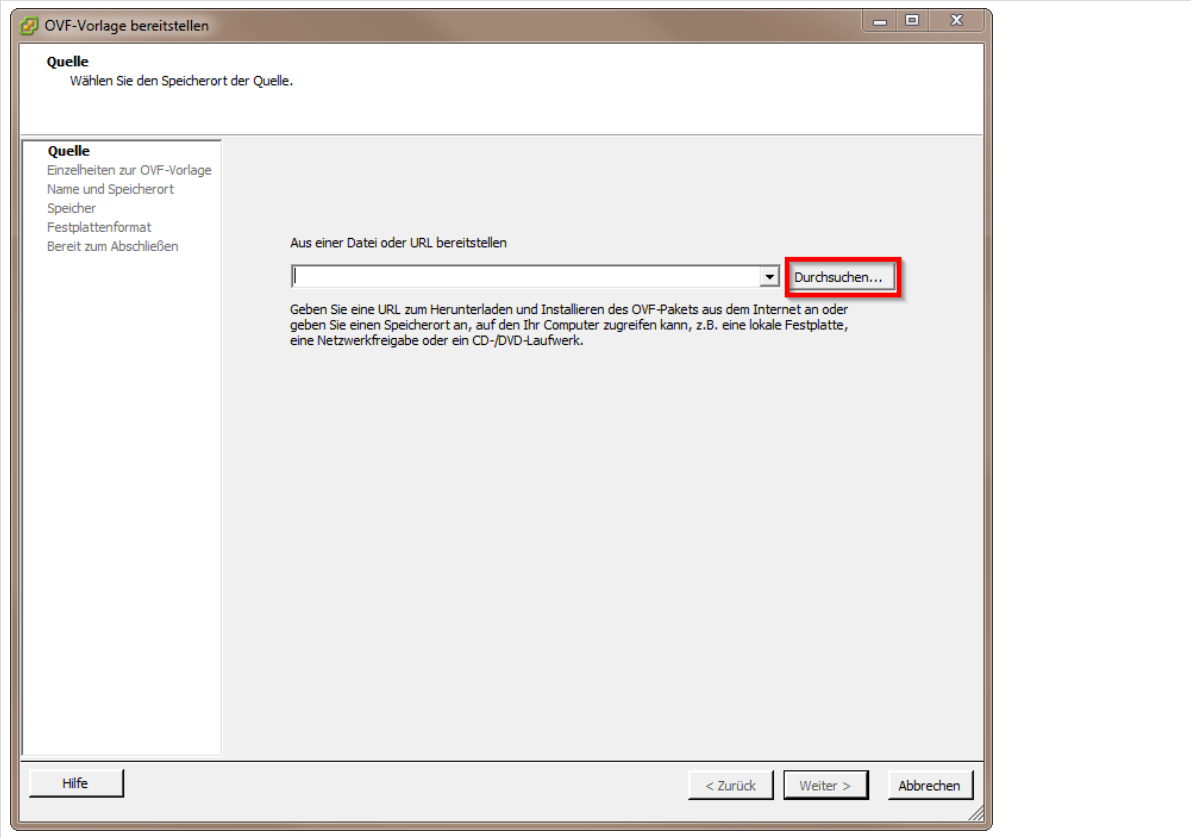

OVF-Vorlage bereitstellen
Quelle
Wählen Sie den Speicherort der Quelle.
Quelle
Einzelheiten zur OVF-Vorlage
Name und Speicherort
Speicher
Festplattenformat
Bereit zum Abschließen
Aus einer Datei oder URL bereitstellen
Durchsuchen...
Geben Sie eine URL zum Herunterladen und Installieren des OVF-Pakets aus dem Internet an oder geben Sie einen Speicherort an, auf den Ihr Computer zugreifen kann, z.B. eine lokale Festplatte, eine Netzwerkfreigabe oder ein CD-/DVD-Laufwerk.
Hilfe
< Zurück
Weiter >
Abbrechen

Abb. 99: Auswahl des Dateipfades für die OVF-Vorlage

Wählen Sie den Pfad zum OVF-Image auf dem *paedML Linux*–Datenträger aus und klicken Sie auf „*Öffnen*“.

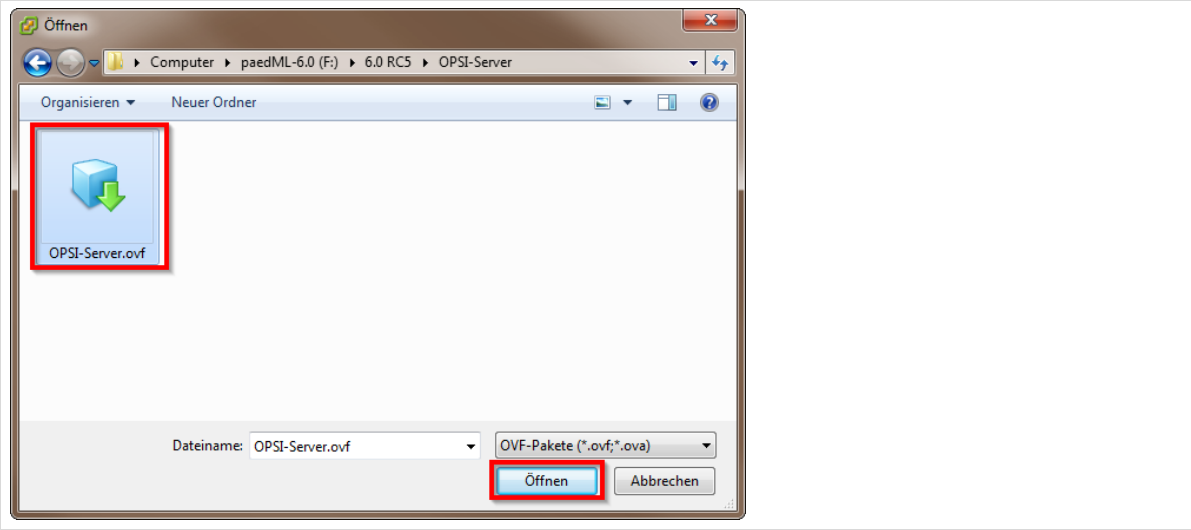


*Abb. 100: Auswahl der OVF-Vorlage für die VM „*opsi-*Server“*

Bestätigen Sie im nächsten Fenster mit „*Weiter*“.

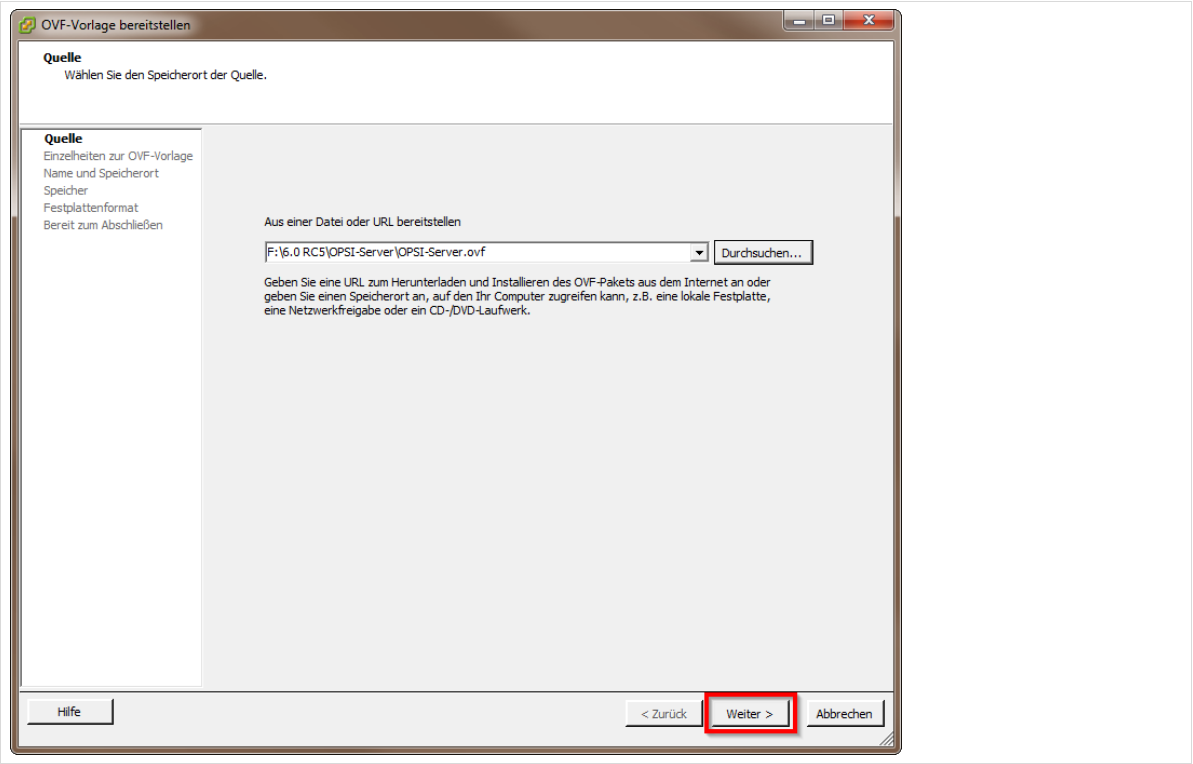

OVF-Vorlage bereitstellen
Quelle
Wählen Sie den Speicherort der Quelle.
Quelle
Einzelheiten zur OVF-Vorlage
Name und Speicherort
Speicher
Festplattenformat
Bereit zum Abschließen
Aus einer Datei oder URL bereitstellen
F:\6.0 RC5\OPSI-Server\OPSI-Server.ovf
Durchsuchen...
Geben Sie eine URL zum Herunterladen und Installieren des OVF-Pakets aus dem Internet an oder geben Sie einen Speicherort an, auf den Ihr Computer zugreifen kann, z.B. eine lokale Festplatte, eine Netzwerkfreigabe oder ein CD-/DVD-Laufwerk.
Hilfe
< Zurück
Weiter >
Abbrechen

*Abb. 101: Der Dateipfad für „*opsi-*Server“ wurde korrekt ausgewählt.*

Anschließend werden einige Informationen zum OVF-Image angezeigt. Klicken Sie auf „*Weiter*“.

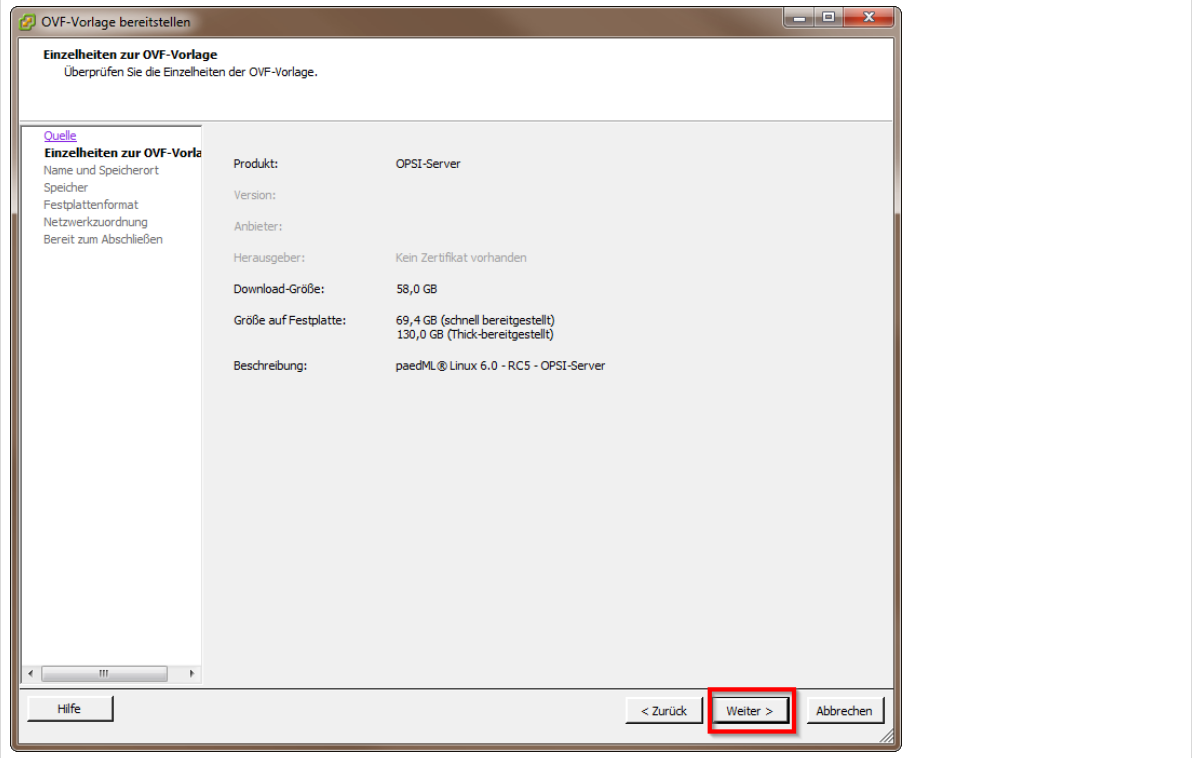


*Abb. 102: Informationen zum OVF-Image „*opsi-*Server“*

Im nächsten Fenster muss die *Endbenutzer-Lizenzvereinbarung* („*EULA*“) durch Klick auf „*Akzeptieren*“ angenommen werden.

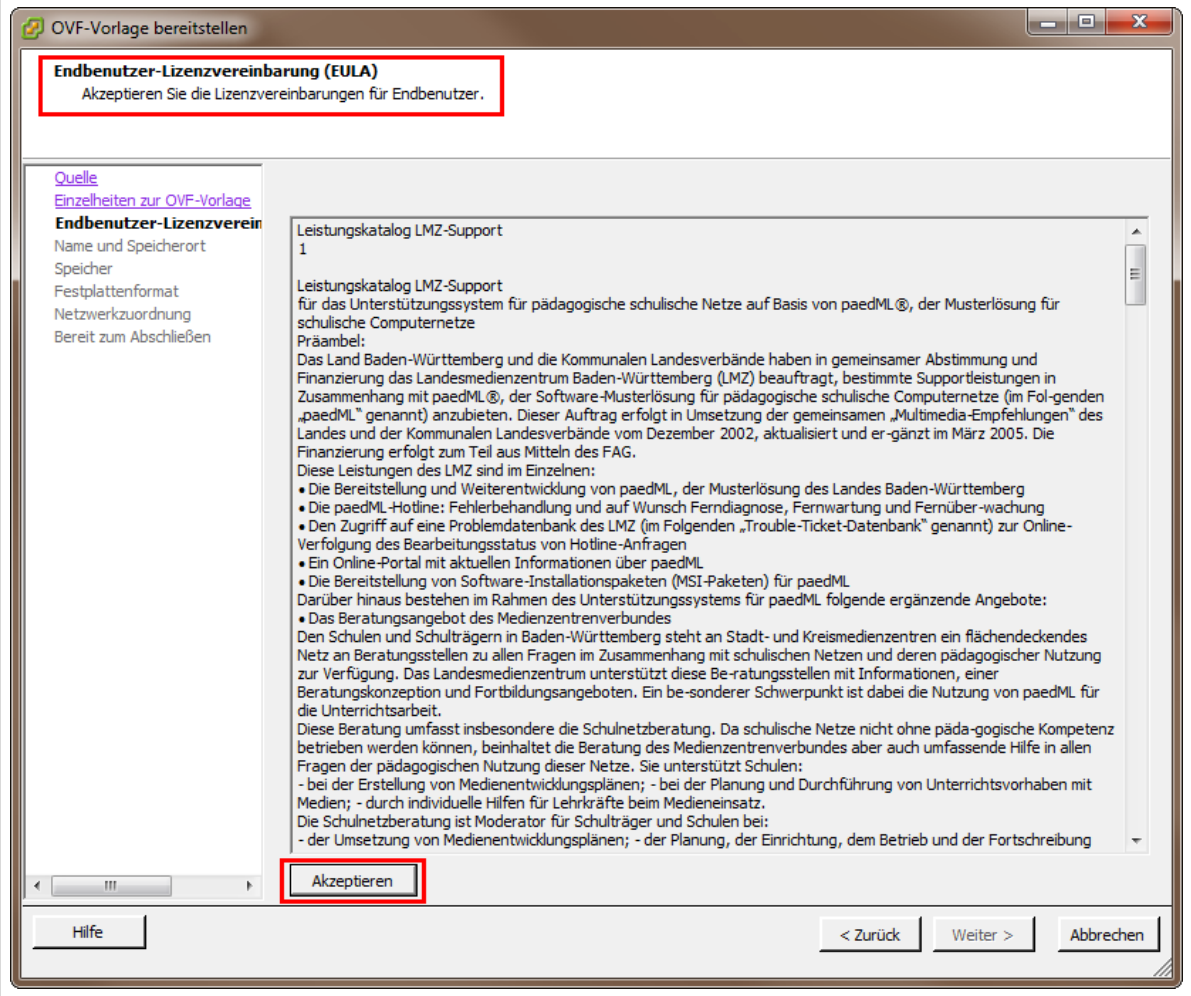

OVF-Vorlage bereitstellen
Endbenutzer-Lizenzvereinbarung (EULA)
Akzeptieren Sie die Lizenzvereinbarungen für Endbenutzer.
Quelle
Einzelheiten zur OVF-Vorlage
Endbenutzer-Lizenzverein
Name und Speicherort
Speicher
Festplattenformat
Netzwerkzuordnung
Bereit zum Abschließen
Leistungskatalog LMZ-Support
1
Leistungskatalog LMZ-Support
für das Unterstützungssystem für pädagogische schulische Netze auf Basis von paedML®, der Musterlösung für schulische Computernetze
Präambel:
Das Land Baden-Württemberg und die Kommunalen Landesverbände haben in gemeinsamer Abstimmung und Finanzierung das Landesmedienzentrum Baden-Württemberg (LMZ) beauftragt, bestimmte Supportleistungen in Zusammenhang mit paedML®, der Software-Musterlösung für pädagogische schulische Computernetze (im Fol-genden „paedML“ genannt) anzubieten. Dieser Auftrag erfolgt in Umsetzung der gemeinsamen „Multimedia-Empfehlungen“ des Landes und der Kommunalen Landesverbände vom Dezember 2002, aktualisiert und er-gänzt im März 2005. Die Finanzierung erfolgt zum Teil aus Mitteln des FAG.
Diese Leistungen des LMZ sind im Einzelnen:
• Die Bereitstellung und Weiterentwicklung von paedML, der Musterlösung des Landes Baden-Württemberg
• Die paedML-Hotline: Fehlerbehandlung und auf Wunsch Ferndiagnose, Fernwartung und Fernüber-wachung
• Den Zugriff auf eine Problemdatenbank des LMZ (im Folgenden „Trouble-Ticket-Datenbank“ genannt) zur Online-Verfolgung des Bearbeitungsstatus von Hotline-Anfragen
• Ein Online-Portal mit aktuellen Informationen über paedML
• Die Bereitstellung von Software-Installationspaketen (MSI-Paketen) für paedML
Darüber hinaus bestehen im Rahmen des Unterstützungssystems für paedML folgende ergänzende Angebote:
• Das Beratungsangebot des Medienzentrenverbundes
Den Schulen und Schulträgern in Baden-Württemberg steht an Stadt- und Kreismedienzentren ein flächendeckendes Netz an Beratungsstellen zu allen Fragen im Zusammenhang mit schulischen Netzen und deren pädagogischer Nutzung zur Verfügung. Das Landesmedienzentrum unterstützt diese Be-ratungsstellen mit Informationen, einer Beratungskonzeption und Fortbildungsangeboten. Ein be-sonderer Schwerpunkt ist dabei die Nutzung von paedML für die Unterrichtsarbeit.
Diese Beratung umfasst insbesondere die Schulnetzberatung. Da schulische Netze nicht ohne päda-gogische Kompetenz betrieben werden können, beinhaltet die Beratung des Medienzentrenverbundes aber auch umfassende Hilfe in allen Fragen der pädagogischen Nutzung dieser Netze. Sie unterstützt Schulen:
- bei der Erstellung von Medienentwicklungsplänen; - bei der Planung und Durchführung von Unterrichtsvorhaben mit Medien; - durch individuelle Hilfen für Lehrkräfte beim Medieneinsatz.
Die Schulnetzberatung ist Moderator für Schulträger und Schulen bei:
- der Umsetzung von Medienentwicklungsplänen; - der Planung, der Einrichtung, dem Betrieb und der Fortschreibung
Akzeptieren
Hilfe
< Zurück
Weiter >
Abbrechen

Abb. 103: Akzeptieren der Endbenutzer-Lizenzvereinbarungen

Klicken Sie danach auf „*Weiter*“:

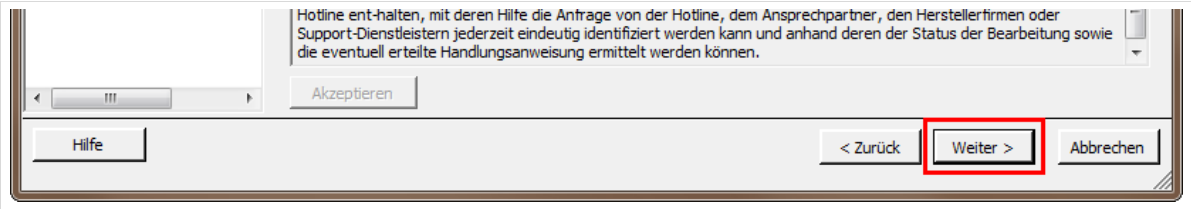

Hotline ent-halten, mit deren Hilfe die Anfrage von der Hotline, dem Ansprechpartner, den Herstellerfirmen oder Support-Dienstleistern jederzeit eindeutig identifiziert werden kann und anhand deren der Status der Bearbeitung sowie die eventuell erteilte Handlungsanweisung ermittelt werden können.
Akzeptieren
Hilfe
< Zurück
Weiter >
Abbrechen

Abb. 104: Die EULA wurde akzeptiert.

Im nachfolgenden Fenster kann ein Name für die virtuelle Maschine angegeben werden. Übernehmen Sie die Voreinstellung „*opsi-Server*“ und klicken Sie auf „*Weiter*“:

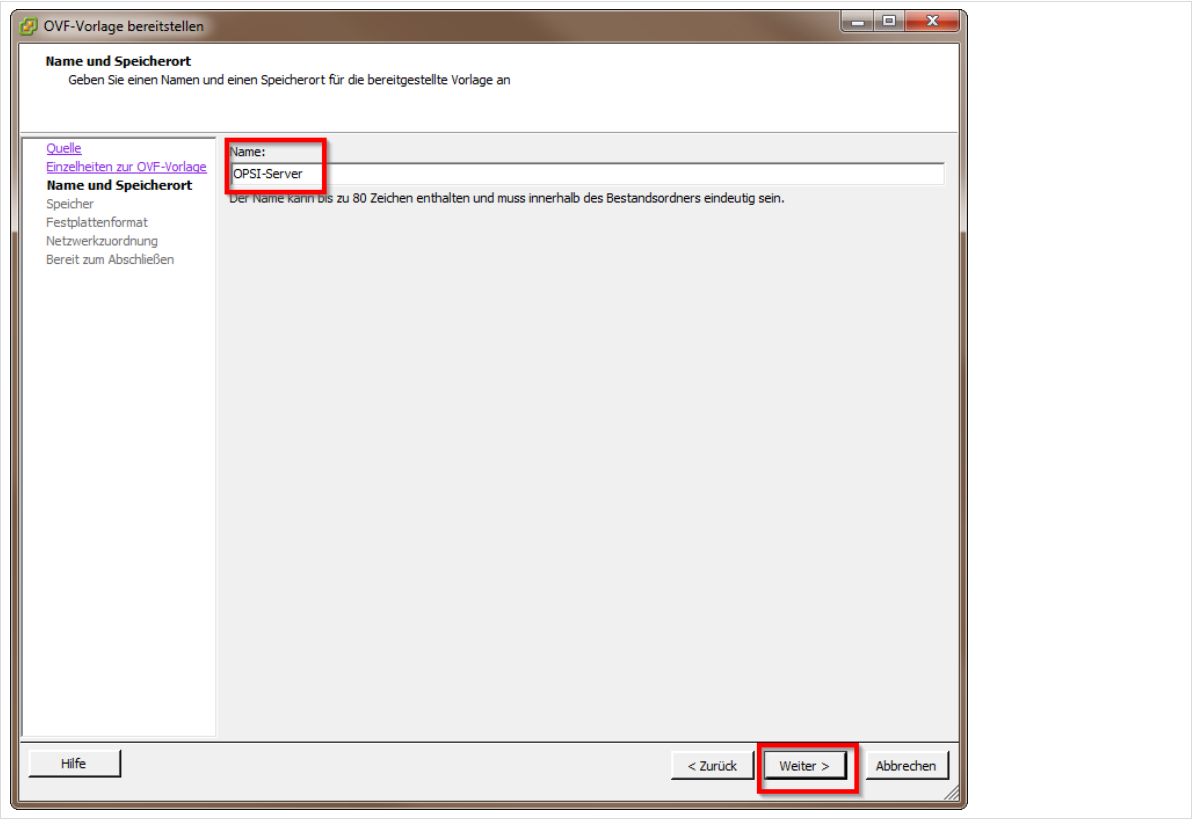


*Abb. 105: Übernehmen des voreingestellten Namens „*opsi-*Server“*

Sollten Sie auf dem Virtualisierungs-Host mehrere Datastores angelegt haben, müssen Sie im nächsten Dialog denjenigen Datastore auswählen, auf dem die virtuelle Maschine gespeichert werden soll. Bestätigen Sie anschließend mit „*Weiter*“.

Falls Sie nur einen einzigen Datastore angelegt haben, wird der folgende Dialog ggf. übersprungen.

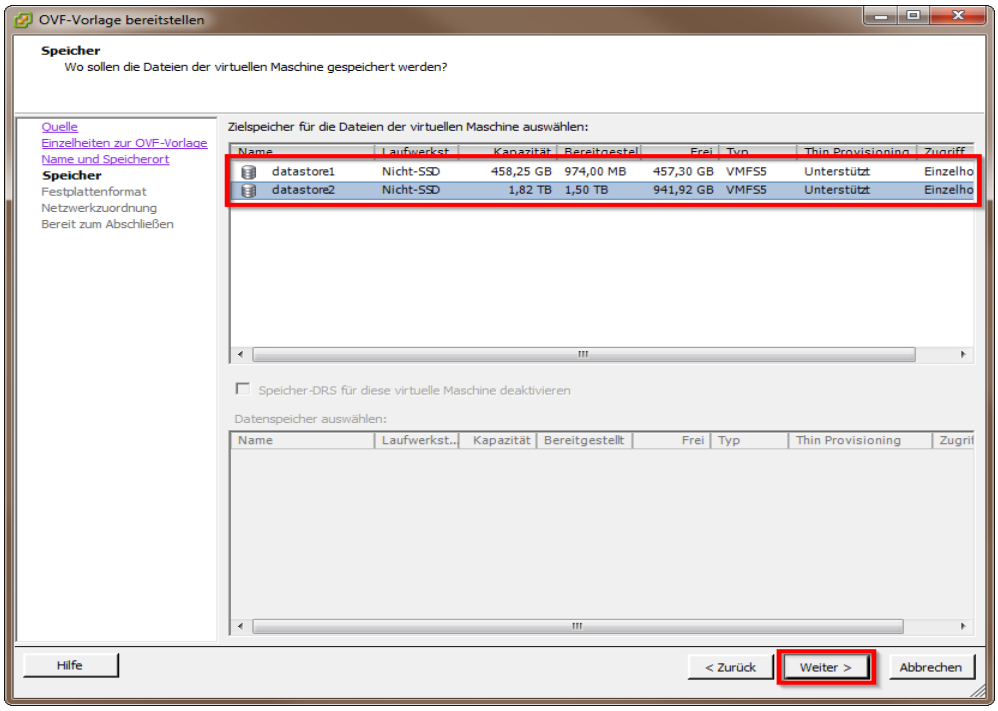


Abb. 106: Auswahl des richtigen Datastores

Im nachfolgenden Dialog wird das Festplattenformat der virtuellen Maschine festgelegt. Wählen Sie die Option „*Thick-Provision Lazy-Zeroed*“ aus und bestätigen Sie mit „*Weiter*“:

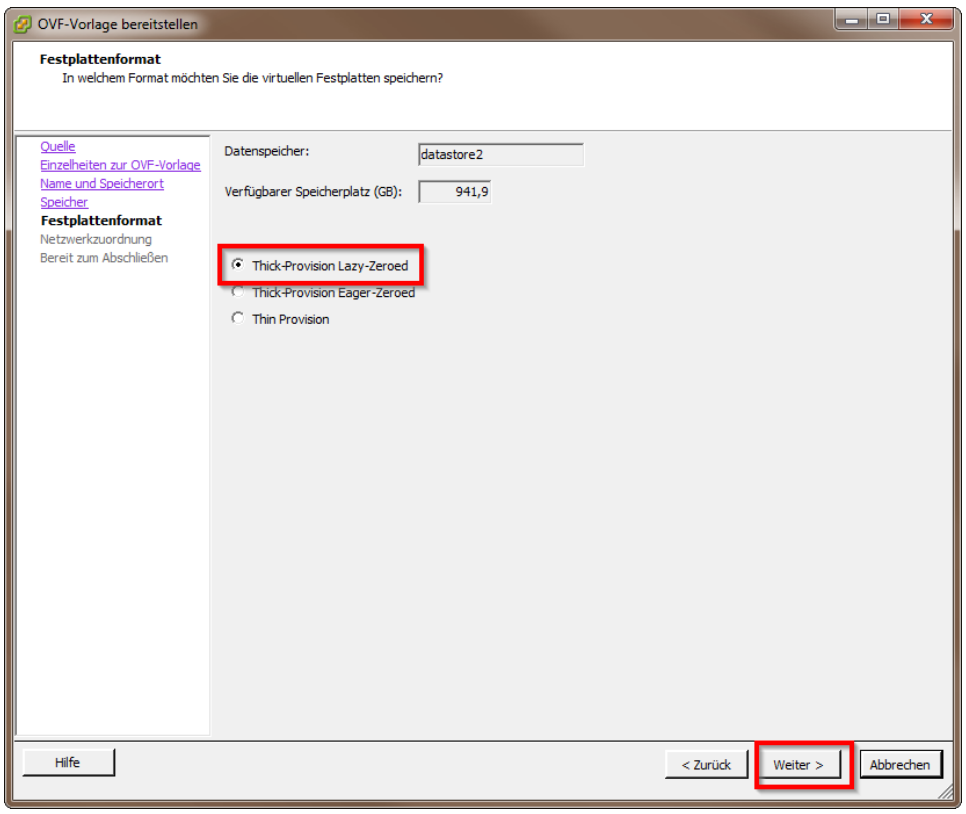


Abb. 107: Auswahl des Festplattenformats „Thick-Provision Lazy-Zeroed“

*Wurden die virtuellen Netzwerke korrekt definiert, so findet die richtige Zuordnung der virtuellen Netzwerkkarte der VM „*opsi-Server*“ automatisch statt. Kontrollieren Sie die Zuordnung und korrigieren Sie diese gegebenenfalls über das Dropdownmenü. Dieses erscheint, wenn Sie auf den im Feld „*Ziellaufwerke*“ vorausgewählten Eintrag klicken. Bestätigen mit „*Weiter*“:*

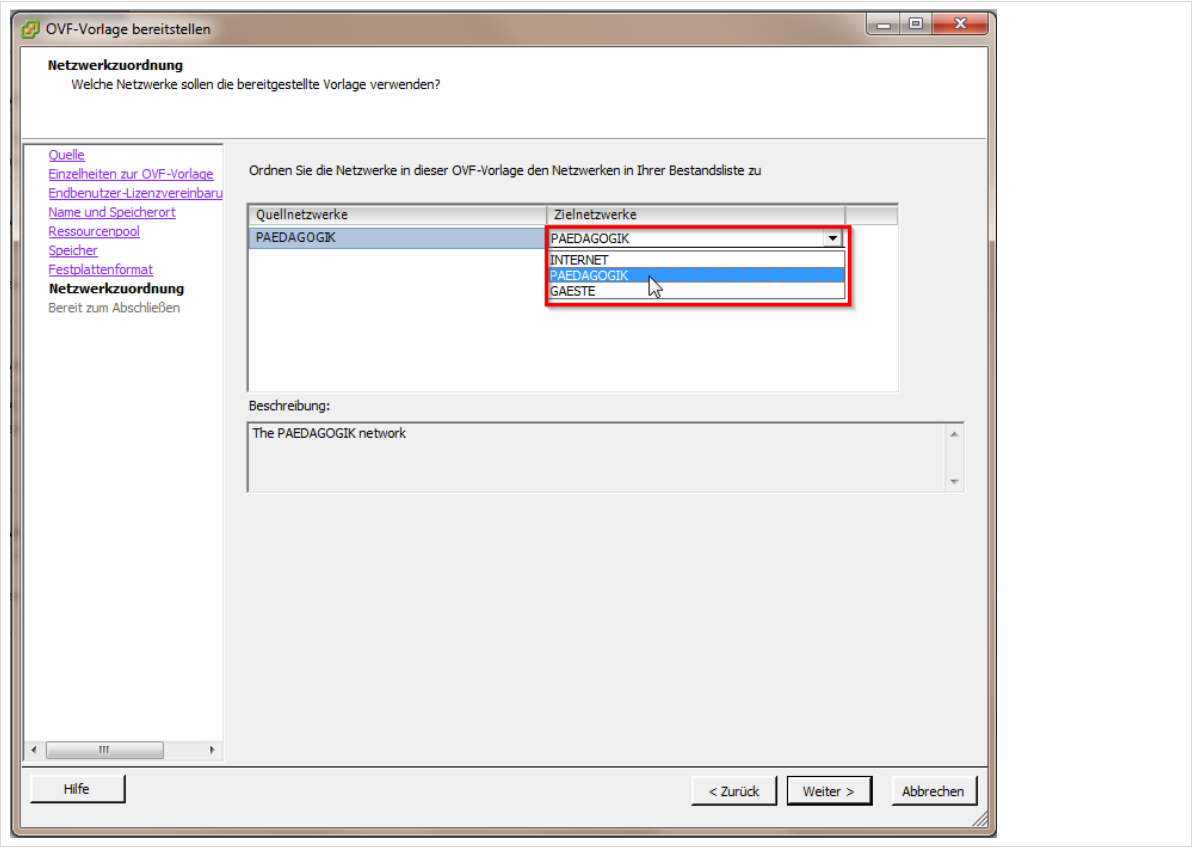


*Abb. 108: Korrekte Zuordnung der virtuellen Netzwerkkarte der VM „*opsi-*Server“ zum Netz „PAEDAGOGIK“.*

Nachfolgend werden nochmals alle Einstellungen angezeigt. Kontrollieren Sie diese Einstellungen und bestätigen Sie den Dialog mit „*Beenden*“:

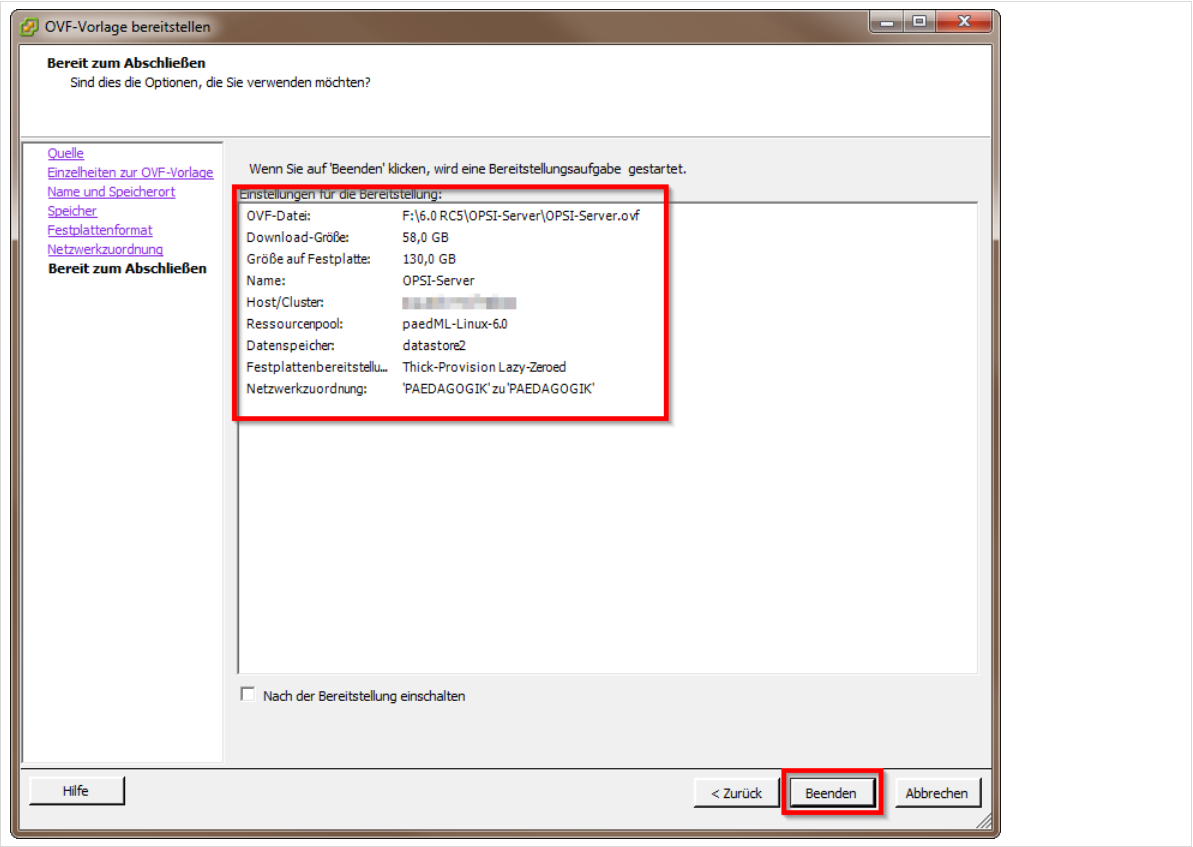


Abb. 109: Kontrolle der Einstellungen vor dem tatsächlichen Importvorgang

Nun beginnt der eigentliche Import der VM, dies kann je nach Systemleistung und Imagegröße einige Zeit in Anspruch nehmen:

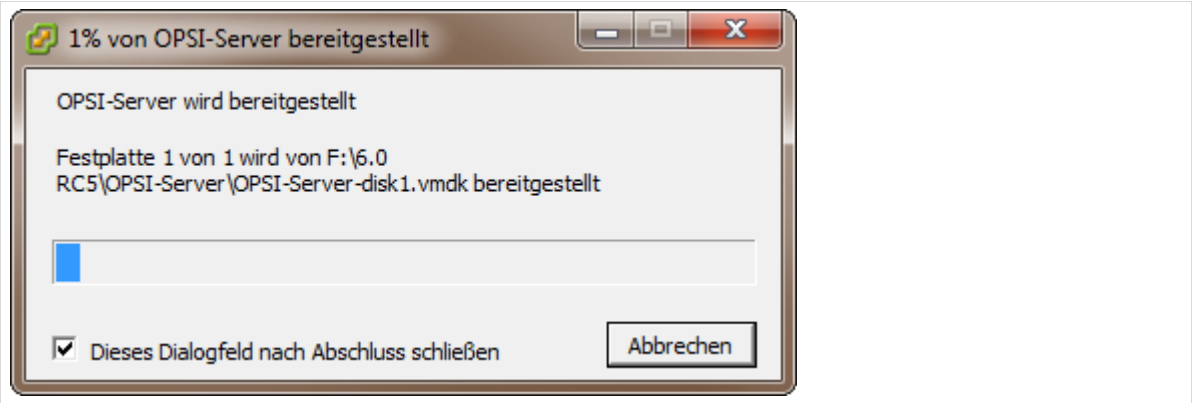

1% von OPSI-Server bereitgestellt
OPSI-Server wird bereitgestellt
Festplatte 1 von 1 wird von F:\6.0 RC5\OPSI-Server\OPSI-Server-disk1.vmdk bereitgestellt
Dieses Dialogfeld nach Abschluss schließen
Abbrechen

Abb. 110: Importvorgang der VM "opsi-Server"

Ein erfolgreicher Import wird wie folgt vom System quittiert, bestätigen Sie mit „*Schließen*“:

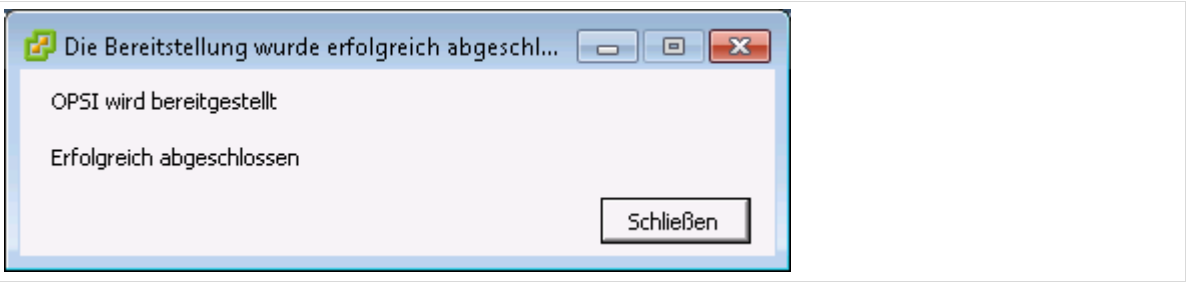


Abb. 111: Die VM „opsi-Server“ wurde erfolgreich importiert.

4.5 Import der VM „AdminVM“

Hinweis: Aus lizenzrechtlichen Gründen darf keine vorkonfigurierte *Windows*-VM ausgeliefert werden, deshalb enthält die VM „*AdminVM*“ nach dem Import noch kein Betriebssystem.

Klicken Sie mit der rechten Maustaste auf den erstellten Ressourcenpool:

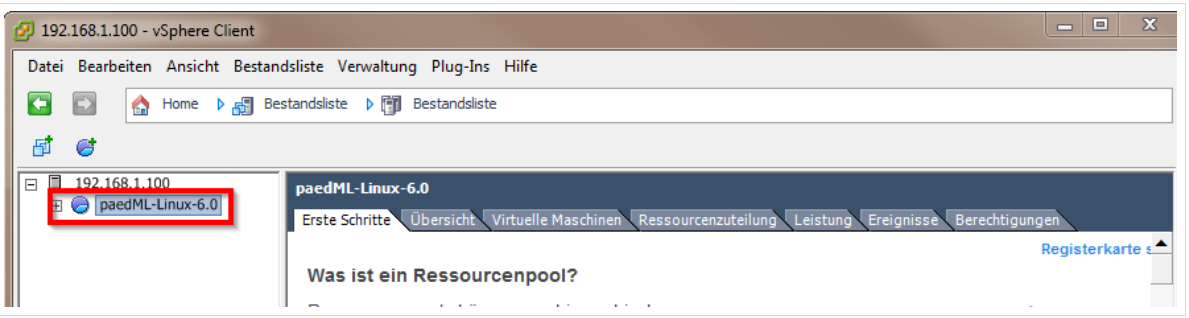


Abb. 112: Auswahl des Ressourcenpools für die „AdminVM“

Wählen Sie den Menüpunkt „*Datei* | *OVF-Vorlage bereitstellen…*“ aus:

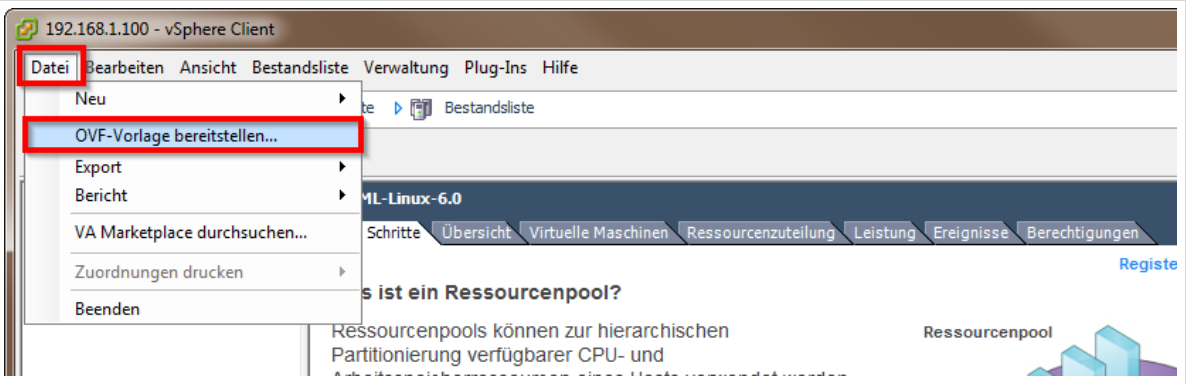


Abb. 113: Import der OVF-Vorlage der „AdminVM“

Im nachfolgend erscheinenden Assistenten klicken Sie zunächst auf „*Durchsuchen*“.

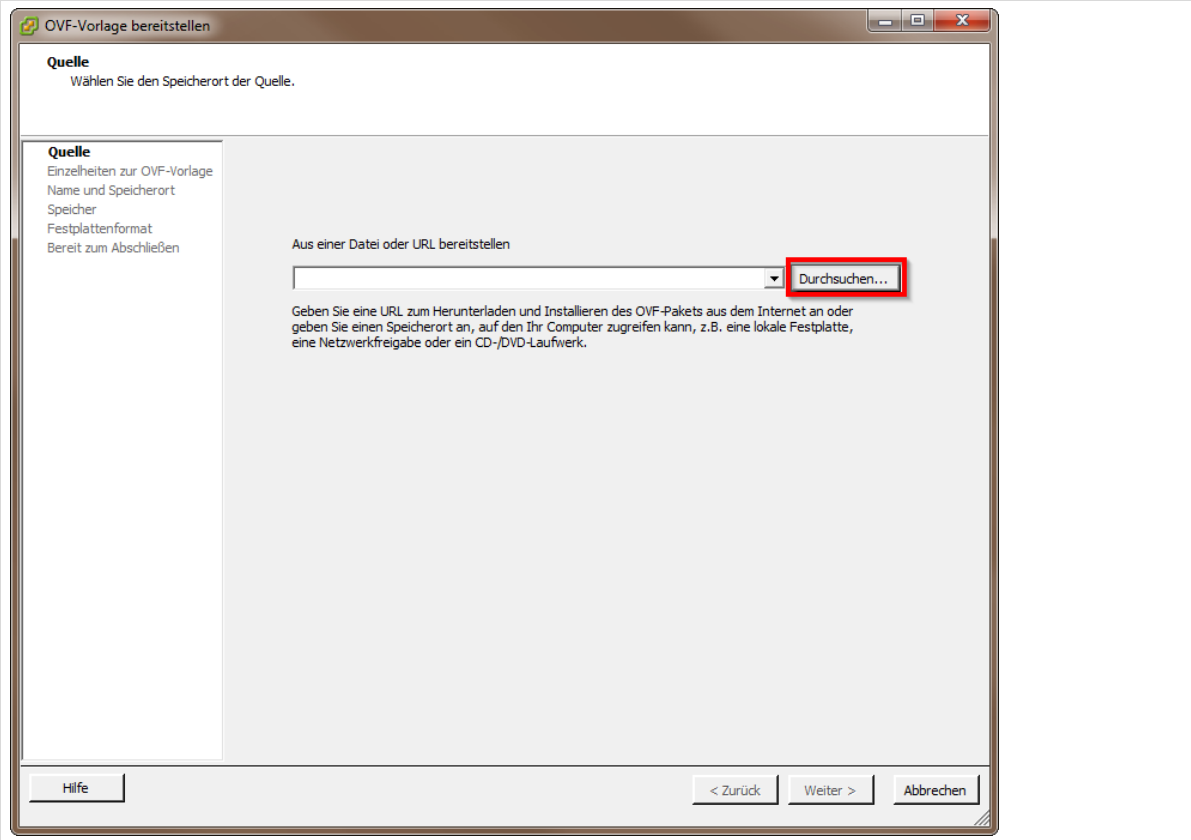

OVF-Vorlage bereitstellen
Quelle
Wählen Sie den Speicherort der Quelle.
Quelle
Einzelheiten zur OVF-Vorlage
Name und Speicherort
Speicher
Festplattenformat
Bereit zum Abschließen
Aus einer Datei oder URL bereitstellen
Durchsuchen...
Geben Sie eine URL zum Herunterladen und Installieren des OVF-Pakets aus dem Internet an oder geben Sie einen Speicherort an, auf den Ihr Computer zugreifen kann, z.B. eine lokale Festplatte, eine Netzwerkfreigabe oder ein CD-/DVD-Laufwerk.
Hilfe
< Zurück
Weiter >
Abbrechen

Abb. 114: Auswahl des Dateipfades der OVF-Vorlage „AdminVM“

Wählen Sie den Pfad zum OVF-Image auf dem *paedML Linux*-Datenträger aus und klicken Sie auf „*Öffnen*“:

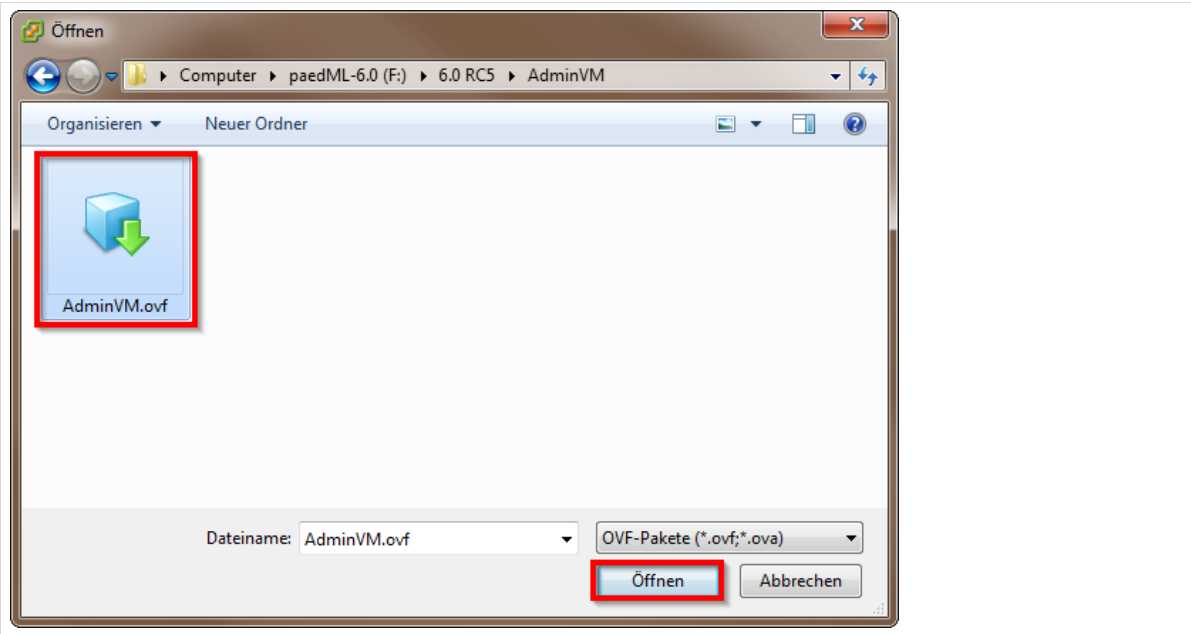


Abb. 115: Auswahl der OVF-Vorlage auf dem Datenträger

Bestätigen Sie im nächsten Fenster mit „*Weiter*“.

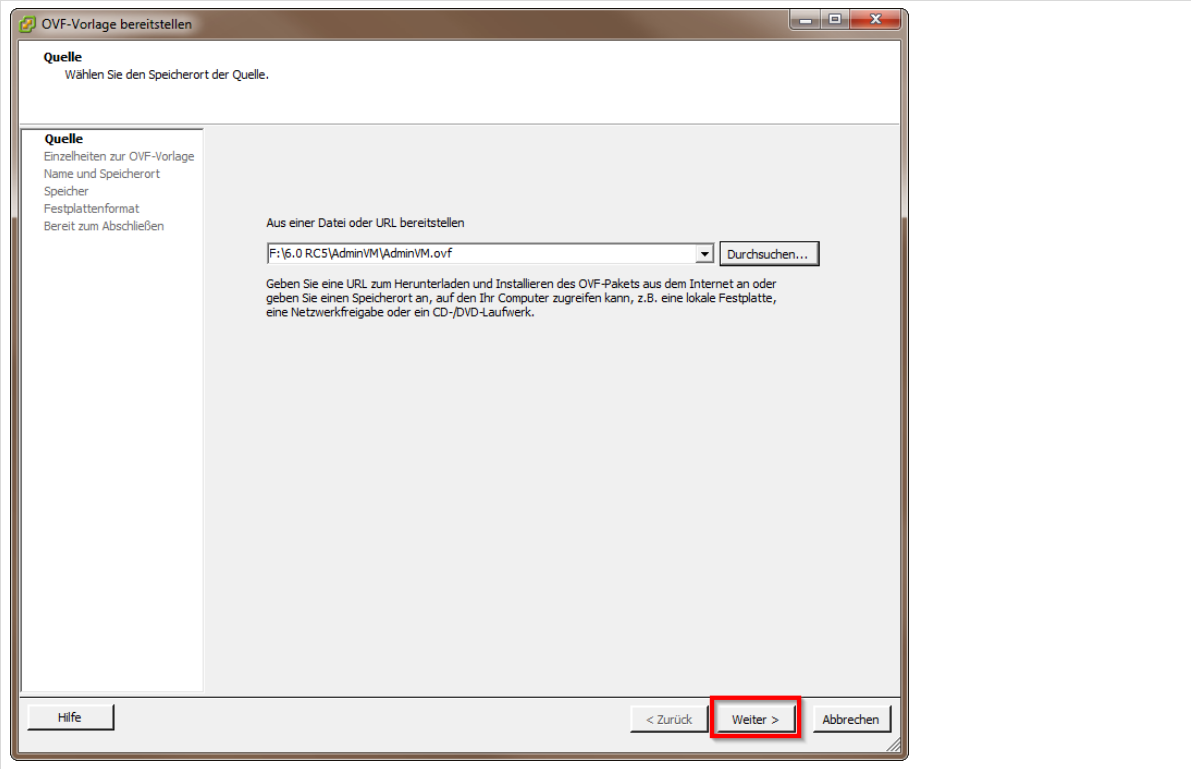

OVF-Vorlage bereitstellen
Quelle
Wählen Sie den Speicherort der Quelle.
Quelle
Einzelheiten zur OVF-Vorlage
Name und Speicherort
Speicher
Festplattenformat
Bereit zum Abschließen
Aus einer Datei oder URL bereitstellen
F:\6.0 RC5\AdminVM\AdminVM.ovf
Durchsuchen...
Geben Sie eine URL zum Herunterladen und Installieren des OVF-Pakets aus dem Internet an oder geben Sie einen Speicherort an, auf den Ihr Computer zugreifen kann, z.B. eine lokale Festplatte, eine Netzwerkfreigabe oder ein CD-/DVD-Laufwerk.
Hilfe
< Zurück
Weiter >
Abbrechen

Abb. 116: Auswahl der OVF-Vorlage

Anschließend werden einige Informationen zum OVF-Image angezeigt. Klicken Sie auf „*Weiter*“.

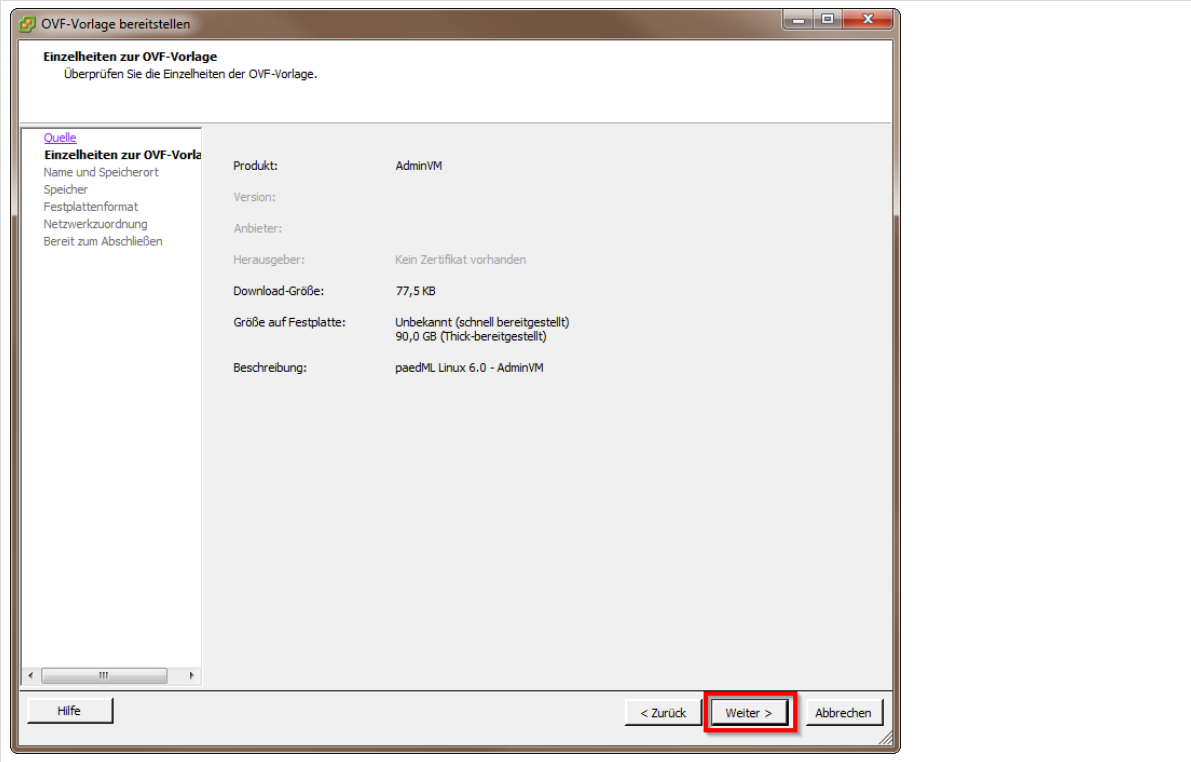


Abb. 117: Details der zu importierenden OVF-Vorlage

Im nächsten Fenster muss die *Endbenutzer-Lizenzvereinbarung* („*EULA*“) durch Klick auf „*Akzeptieren*“ angenommen werden.

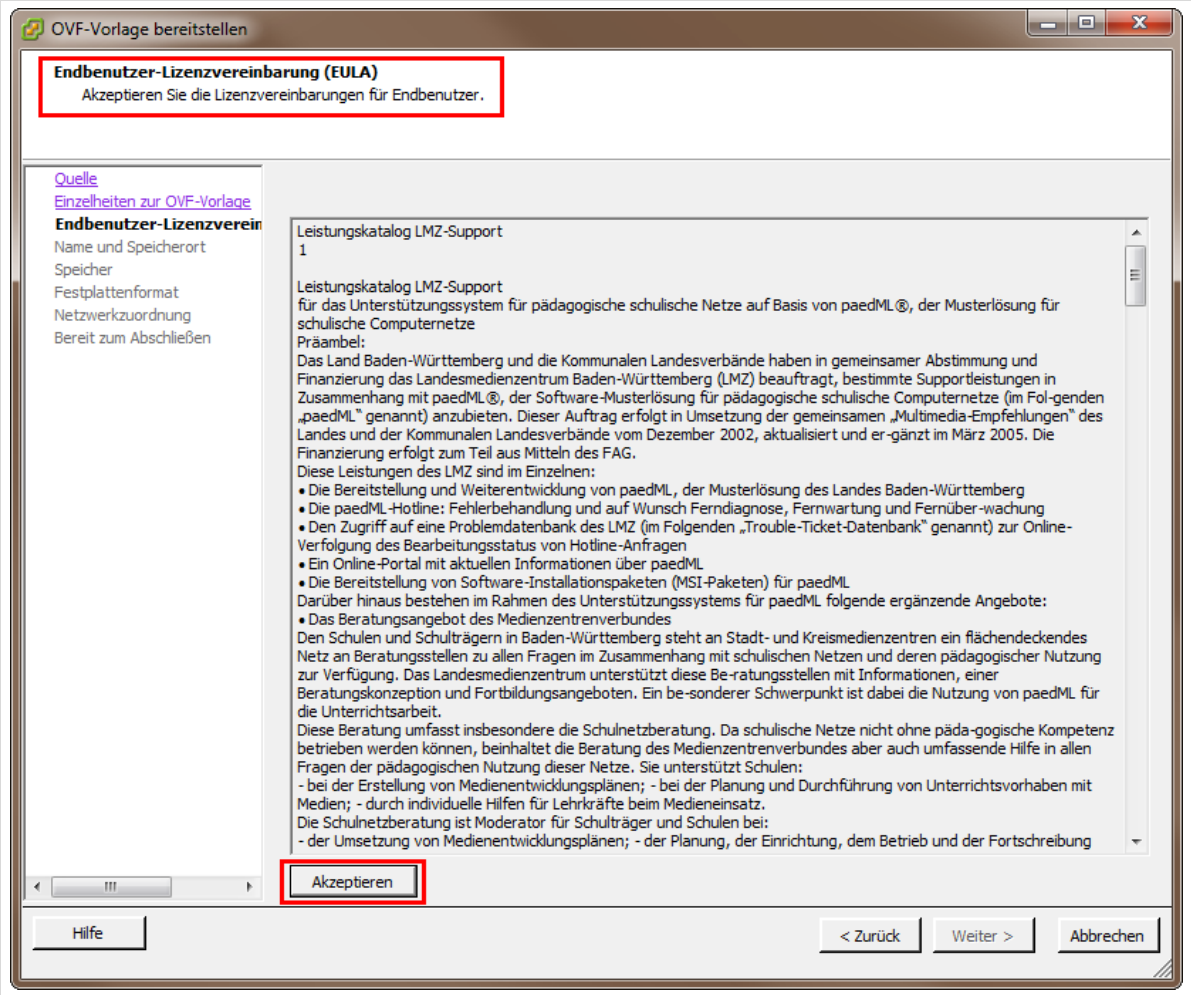

OVF-Vorlage bereitstellen
Endbenutzer-Lizenzvereinbarung (EULA)
Akzeptieren Sie die Lizenzvereinbarungen für Endbenutzer.
Quelle
Einzelheiten zur OVF-Vorlage
Endbenutzer-Lizenzverein
Name und Speicherort
Speicher
Festplattenformat
Netzwerkzuordnung
Bereit zum Abschließen
Leistungskatalog LMZ-Support
1
Leistungskatalog LMZ-Support
für das Unterstützungssystem für pädagogische schulische Netze auf Basis von paedML®, der Musterlösung für schulische Computernetze
Präambel:
Das Land Baden-Württemberg und die Kommunalen Landesverbände haben in gemeinsamer Abstimmung und Finanzierung das Landesmedienzentrum Baden-Württemberg (LMZ) beauftragt, bestimmte Supportleistungen in Zusammenhang mit paedML®, der Software-Musterlösung für pädagogische schulische Computernetze (im Fol-genden „paedML“ genannt) anzubieten. Dieser Auftrag erfolgt in Umsetzung der gemeinsamen „Multimedia-Empfehlungen“ des Landes und der Kommunalen Landesverbände vom Dezember 2002, aktualisiert und er-gänzt im März 2005. Die Finanzierung erfolgt zum Teil aus Mitteln des FAG.
Diese Leistungen des LMZ sind im Einzelnen:
• Die Bereitstellung und Weiterentwicklung von paedML, der Musterlösung des Landes Baden-Württemberg
• Die paedML-Hotline: Fehlerbehandlung und auf Wunsch Ferndiagnose, Fernwartung und Fernüber-wachung
• Den Zugriff auf eine Problemdatenbank des LMZ (im Folgenden „Trouble-Ticket-Datenbank“ genannt) zur Online-Verfolgung des Bearbeitungsstatus von Hotline-Anfragen
• Ein Online-Portal mit aktuellen Informationen über paedML
• Die Bereitstellung von Software-Installationspaketen (MSI-Paketen) für paedML
Darüber hinaus bestehen im Rahmen des Unterstützungssystems für paedML folgende ergänzende Angebote:
• Das Beratungsangebot des Medienzentrenverbundes
Den Schulen und Schulträgern in Baden-Württemberg steht an Stadt- und Kreismedienzentren ein flächendeckendes Netz an Beratungsstellen zu allen Fragen im Zusammenhang mit schulischen Netzen und deren pädagogischer Nutzung zur Verfügung. Das Landesmedienzentrum unterstützt diese Be-ratungsstellen mit Informationen, einer Beratungskonzeption und Fortbildungsangeboten. Ein be-sonderer Schwerpunkt ist dabei die Nutzung von paedML für die Unterrichtsarbeit.
Diese Beratung umfasst insbesondere die Schulnetzberatung. Da schulische Netze nicht ohne päda-gogische Kompetenz betrieben werden können, beinhaltet die Beratung des Medienzentrenverbundes aber auch umfassende Hilfe in allen Fragen der pädagogischen Nutzung dieser Netze. Sie unterstützt Schulen:
- bei der Erstellung von Medienentwicklungsplänen; - bei der Planung und Durchführung von Unterrichtsvorhaben mit Medien; - durch individuelle Hilfen für Lehrkräfte beim Medieneinsatz.
Die Schulnetzberatung ist Moderator für Schulträger und Schulen bei:
- der Umsetzung von Medienentwicklungsplänen; - der Planung, der Einrichtung, dem Betrieb und der Fortschreibung
Akzeptieren
Hilfe
< Zurück
Weiter >
Abbrechen

Abb. 118: Akzeptieren der Endbenutzer-Lizenzvereinbarungen

Klicken Sie danach auf „*Weiter*“:

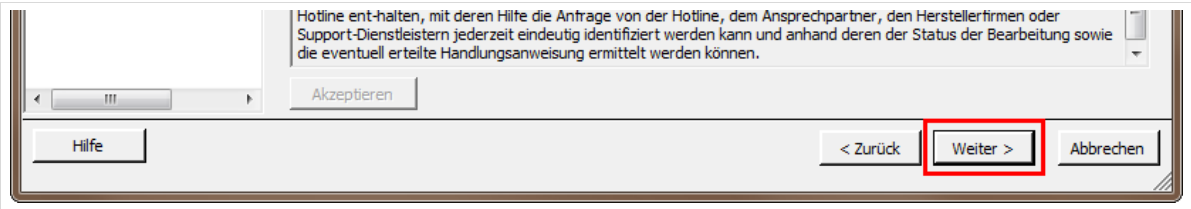

Hotline ent-halten, mit deren Hilfe die Anfrage von der Hotline, dem Ansprechpartner, den Herstellerfirmen oder Support-Dienstleistern jederzeit eindeutig identifiziert werden kann und anhand deren der Status der Bearbeitung sowie die eventuell erteilte Handlungsanweisung ermittelt werden können.
Akzeptieren
Hilfe
< Zurück
Weiter >
Abbrechen

Abb. 119: Die EULA wurde akzeptiert.

Im nachfolgenden Fenster kann ein Name für die virtuelle Maschine angegeben werden. Übernehmen Sie die Voreinstellung „*AdminVM*“ und klicken Sie auf „*Weiter*“.

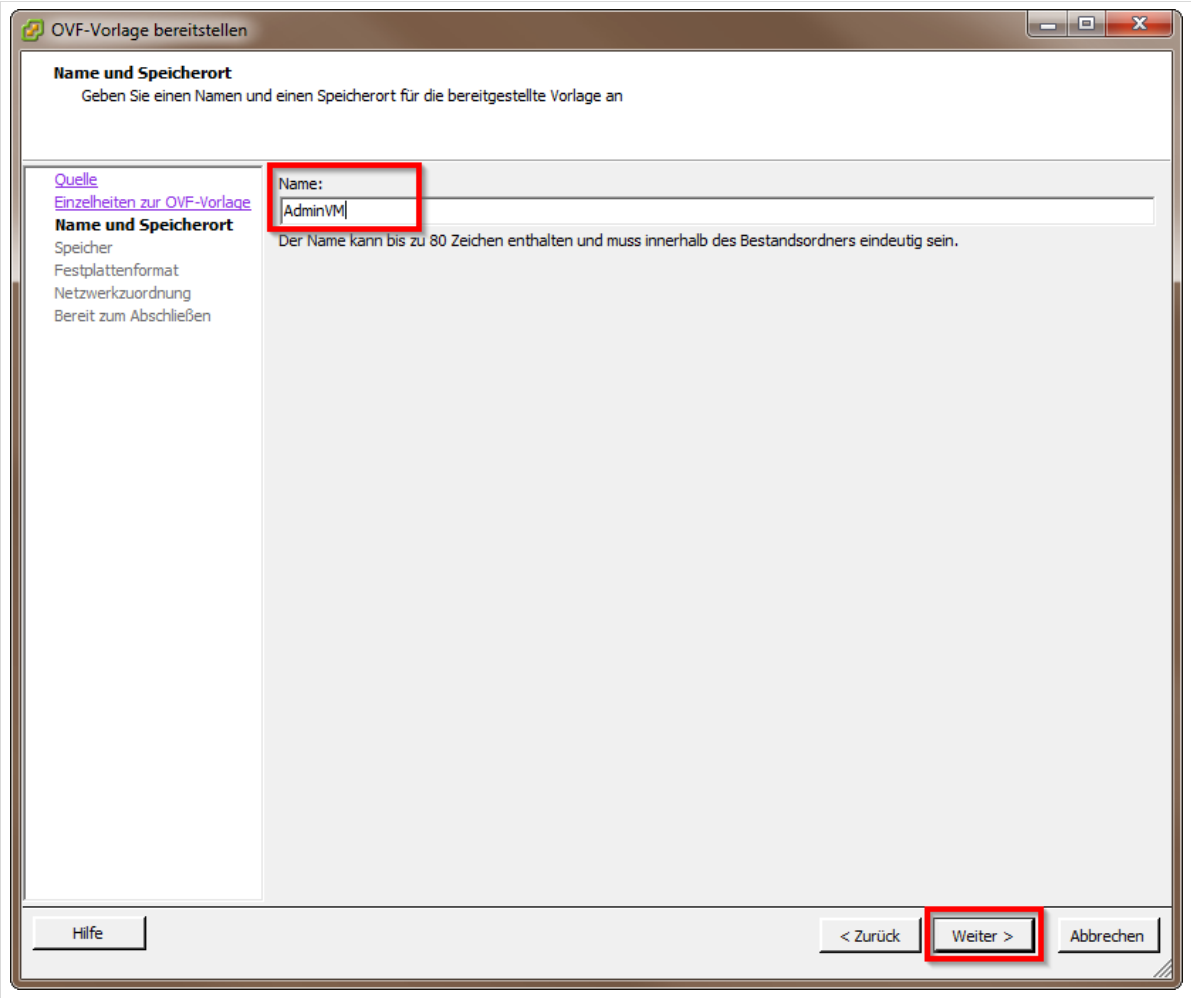


Abb. 120: Festlegen des Namens der VM „AdminVM“

Sollten Sie auf dem Virtualisierungs-Host mehrere Datastores angelegt haben, müssen Sie im nächsten Dialog denjenigen Datastore auswählen, auf dem die virtuelle Maschine gespeichert werden soll. Bestätigen Sie anschließend mit „*Weiter*“.

Falls Sie nur einen einzigen Datastore angelegt haben, wird der folgende Dialog übersprungen.

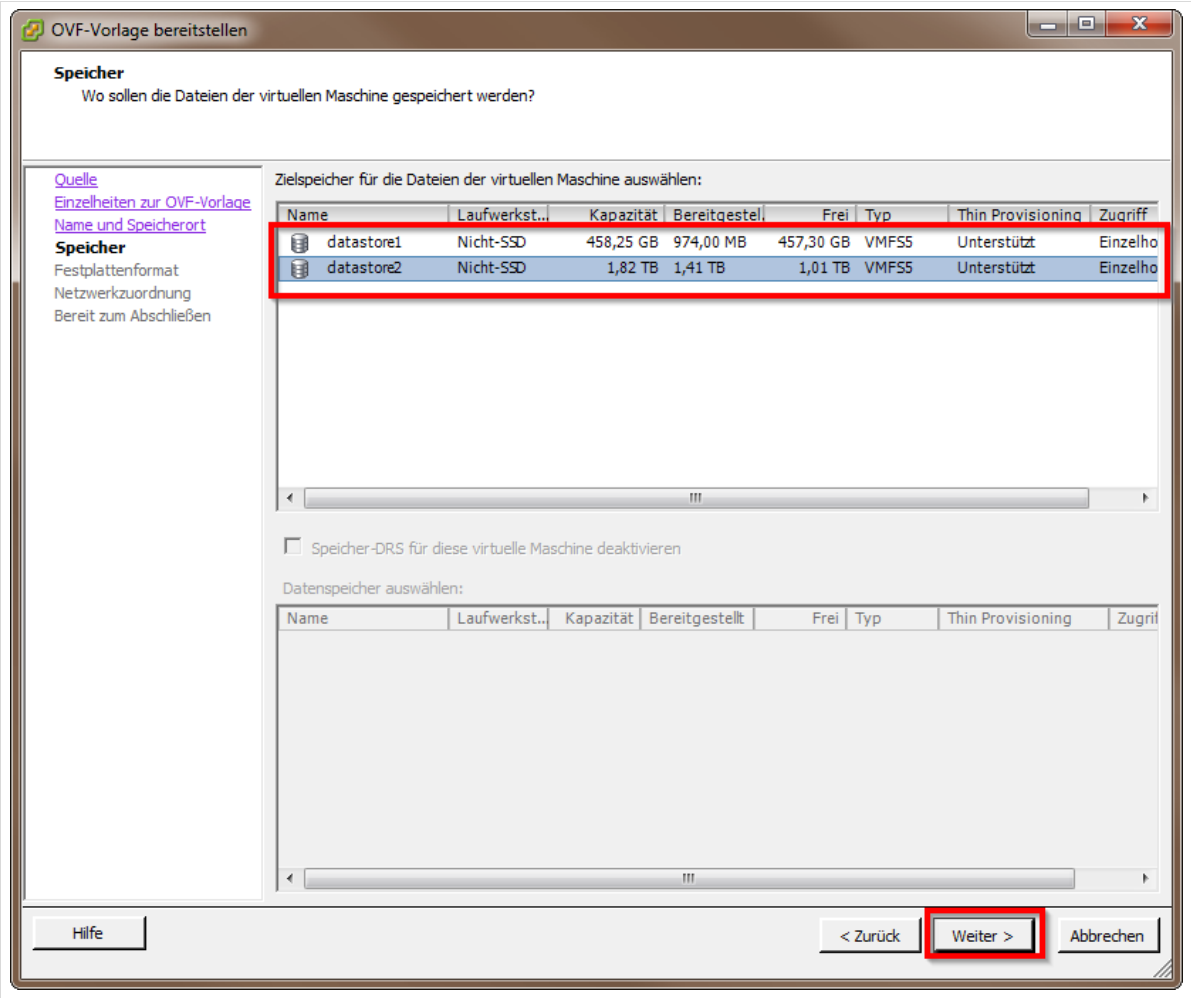


Abb. 121: Auswahl des Datastores

Im nachfolgenden Dialog wird das Festplattenformat der virtuellen Maschine festgelegt. Wählen Sie die Option „*Thick-Provision Lazy-Zeroed*“ aus und bestätigen Sie mit „*Weiter*“.

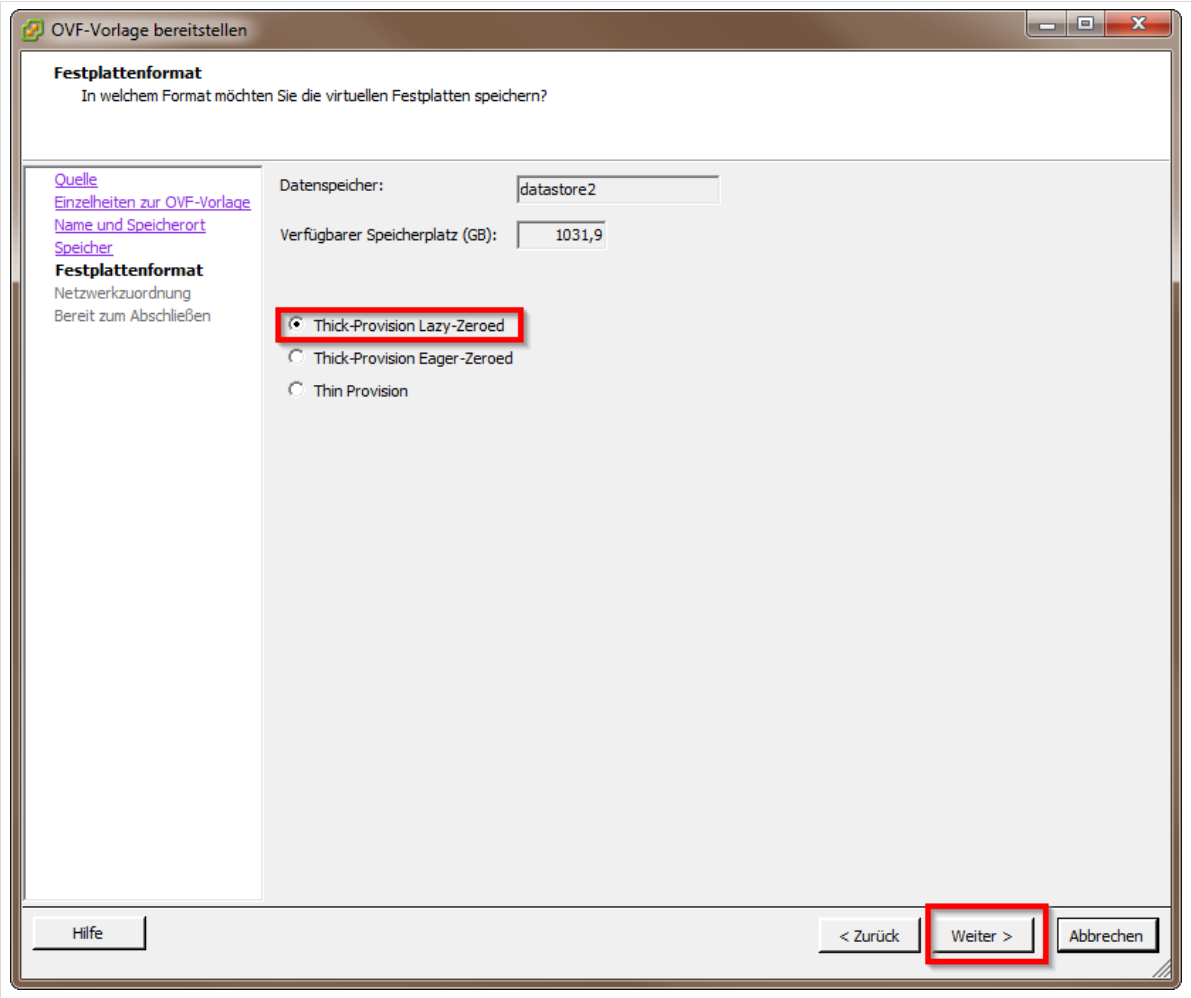


Abb. 122: Festlegen der Provisionierungs-Art „Thick-Provision Lazy-Zeroed“.

Kontrollieren Sie im nächsten Fenster, ob die Zuordnung ins Netz „*PAEDAGOGIK*“ korrekt ist. Korrigieren Sie die Zuordnung gegebenenfalls über das Dropdownmenü. Dieses erscheint, wenn Sie auf den im Feld „*Ziellaufwerke*“ vorausgewählten Eintrag klicken. Bestätigen mit „*Weiter*“:

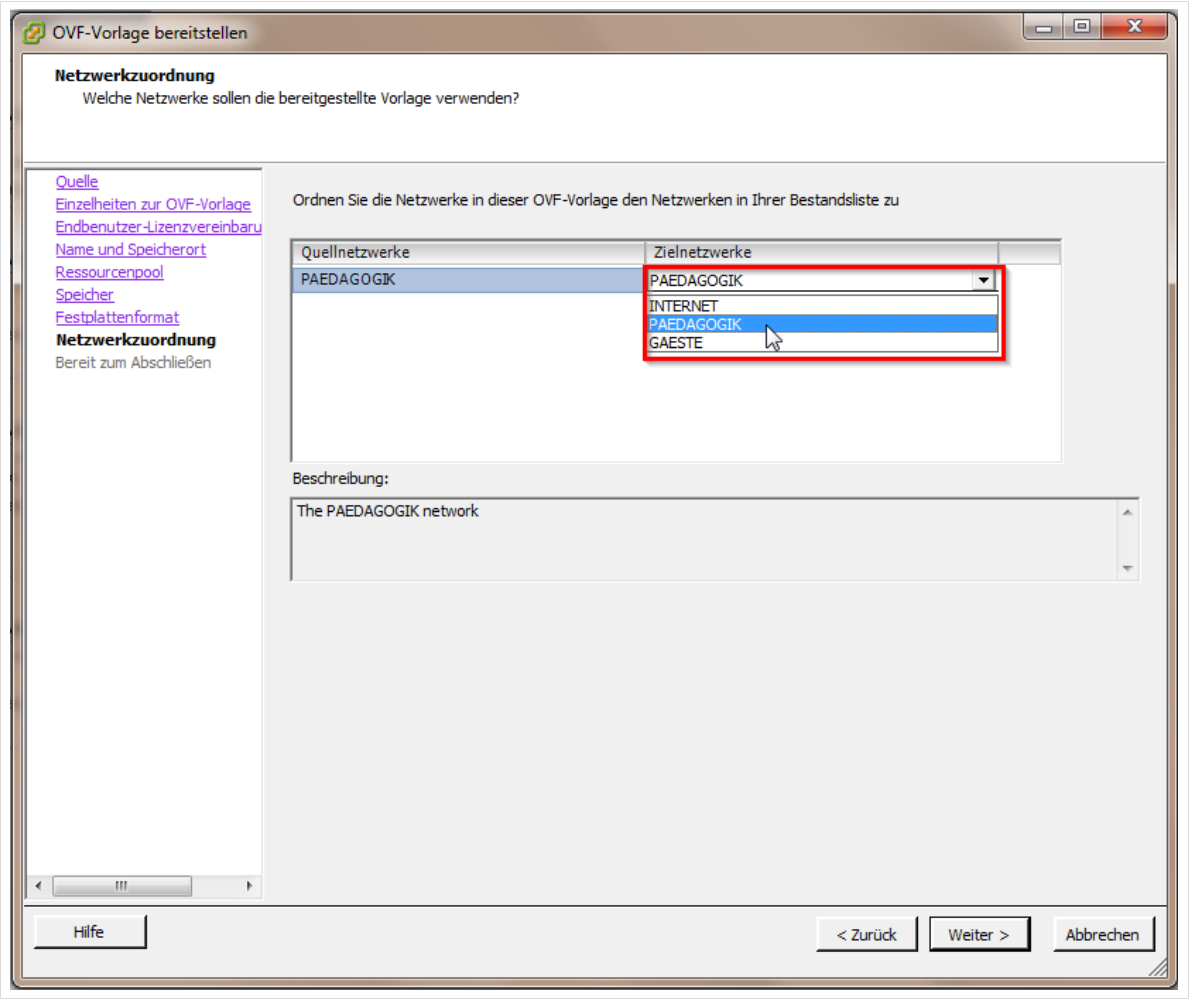


Abb. 123: Zuordnung der Netzwerkkarte ins Netz „PAEDAGOGIK“.

Vor dem endgültigen Import werden alle Einstellungen in einer Übersichtsseite dargestellt. Überprüfen Sie die Einstellungen und klicken Sie auf „*Beenden*“.

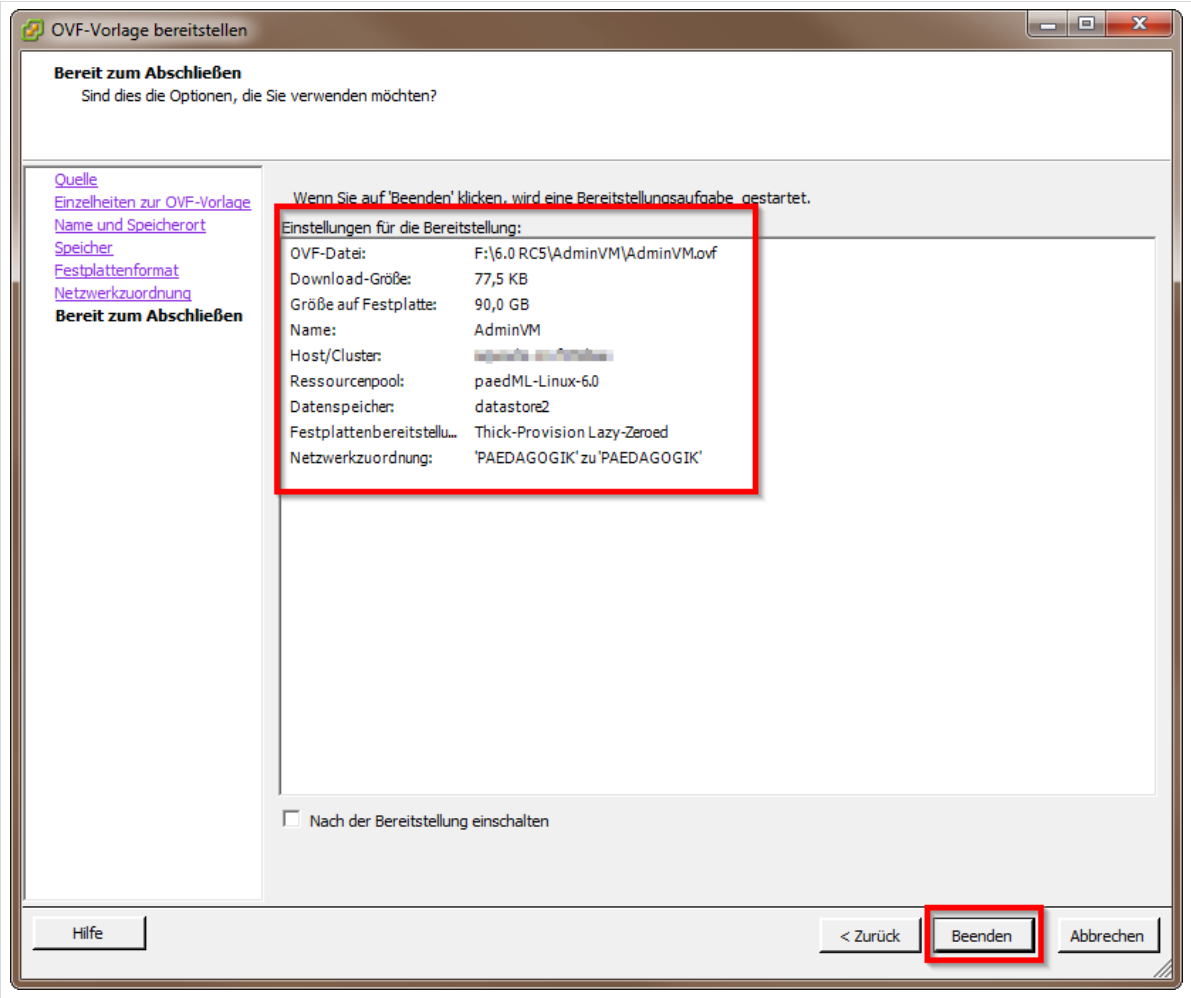


Abb. 124: Überprüfen aller Einstellungen vor dem Import

Daraufhin wird die virtuelle Maschine importiert. Da die Festplatte der VM noch kein Betriebssystem enthält, benötigt der Importvorgang nur kurze Zeit:

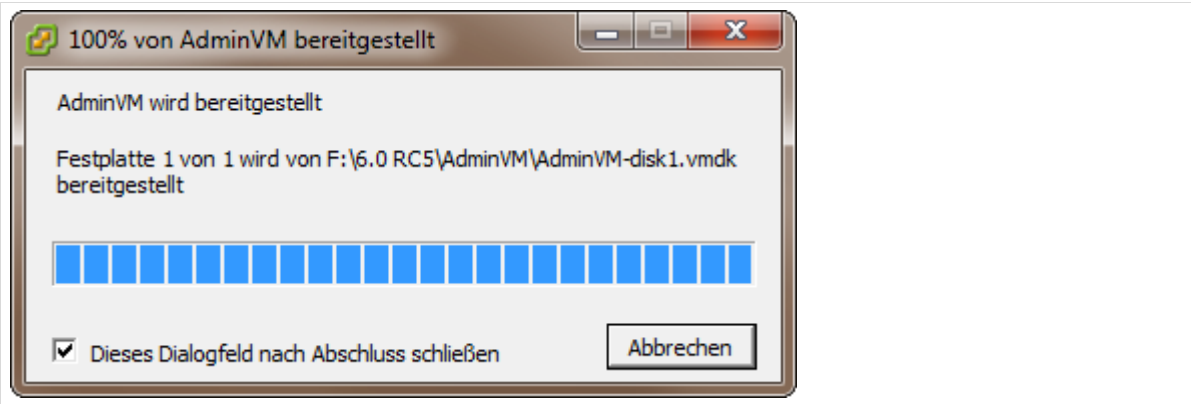

100% von AdminVM bereitgestellt
AdminVM wird bereitgestellt
Festplatte 1 von 1 wird von F:\6.0 RC5\AdminVM\AdminVM-disk1.vmdk bereitgestellt
Dieses Dialogfeld nach Abschluss schließen
Abbrechen

Abb. 125: Import der virtuellen Maschine „AdminVM“ benötigt nur wenig Zeit

4.6 Überprüfen des Imports

Sind alle virtuellen Maschinen erfolgreich importiert, so sollten Sie am Ende im *vSphere-Client* folgendes Bild vorfinden:

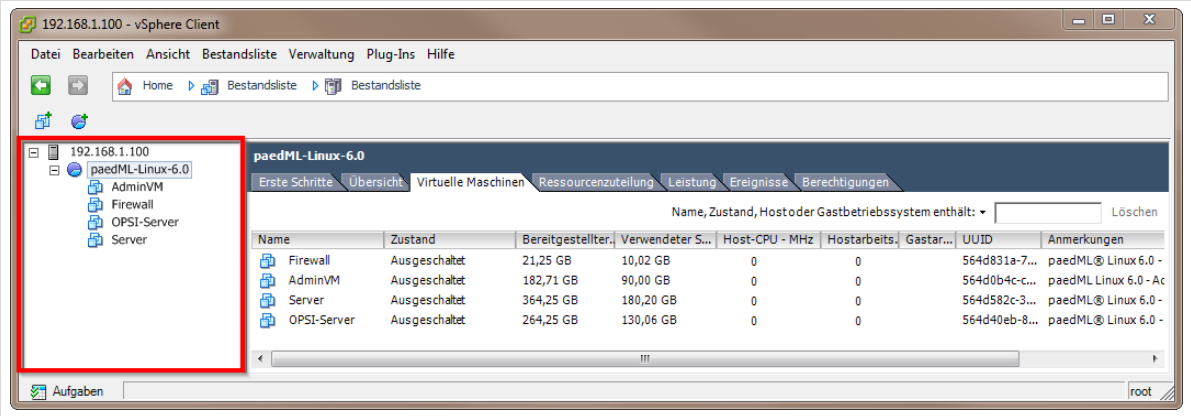

192.168.1.100 - vSphere Client
Datei Bearbeiten Ansicht Bestandsliste Verwaltung Plug-Ins Hilfe
Home Bestandsliste Bestandsliste
192.168.1.100
paedML-Linux-6.0
AdminVM
Firewall
OPSI-Server
Server
paedML-Linux-6.0
Erste Schritte Übersicht Virtuelle Maschinen Ressourcenzuteilung Leistung Ereignisse Berechtigungen
Name, Zustand, Host oder Gastbetriebssystem enthält: Löschen
Name Zustand Bereitgestellter... Verwendeter S... Host-CPU - MHz Hostarbeits... Gastar... UUID Anmerkungen
Firewall Ausgeschaltet 21,25 GB 10,02 GB 0 0 564d831a-7... paedML® Linux 6.0 -
AdminVM Ausgeschaltet 182,71 GB 90,00 GB 0 0 564d0b4c-c... paedML Linux 6.0 - Ac
Server Ausgeschaltet 364,25 GB 180,20 GB 0 0 564d582c-3... paedML® Linux 6.0 -
OPSI-Server Ausgeschaltet 264,25 GB 130,06 GB 0 0 564d40eb-8... paedML® Linux 6.0 -
Aufgaben
root

Abb. 126: Alle virtuellen Maschinen wurden erfolgreich in den Ressourcenpool importiert.

Überprüfen Sie den erfolgreichen Import der einzelnen virtuellen Maschinen, indem Sie diese per Mausklick im *vSphere-Client* anwählen. Die Übersichtsseiten im Auslieferungszustand sind auf den nächsten Seiten dargestellt.

Übersichtsseite der VM „Firewall“

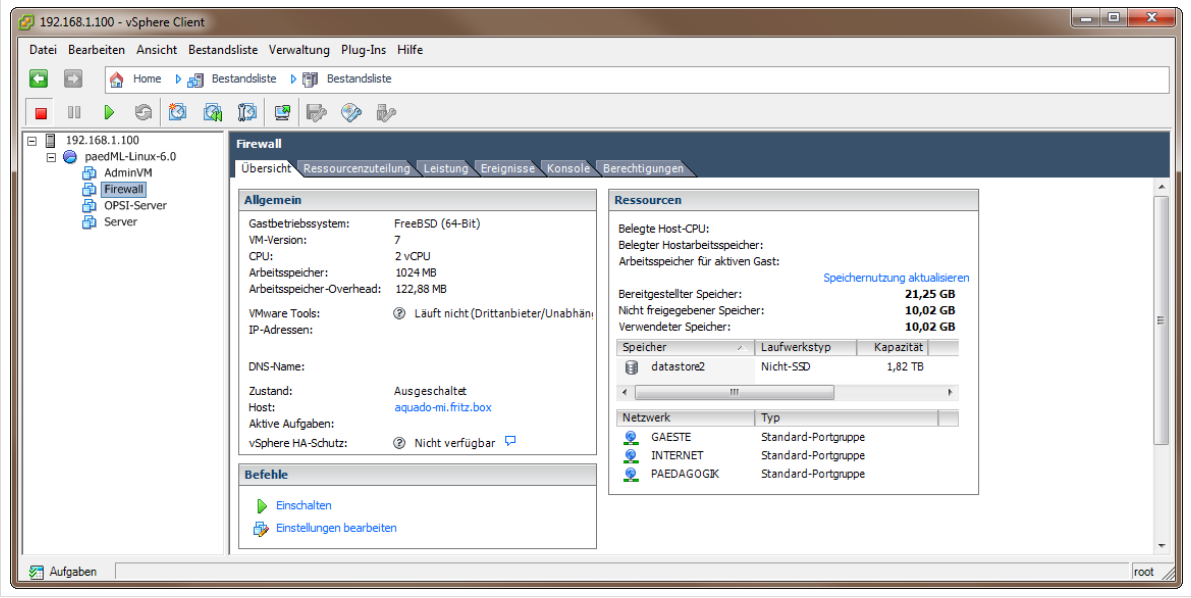


Abb. 127: Übersichtsseite der VM „Firewall“ im Auslieferungszustand

Übersichtsseite VM „Server“

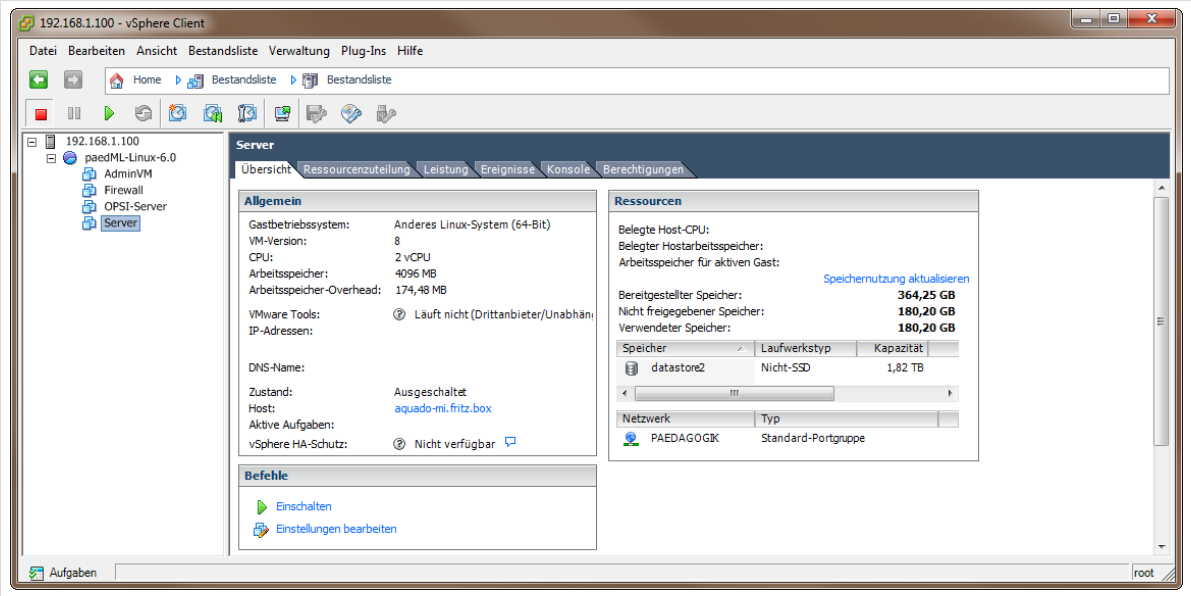


Abb. 128: Übersichtsseite der VM „Server“ im Auslieferungszustand

Übersichtsseite VM „*opsi*-Server“

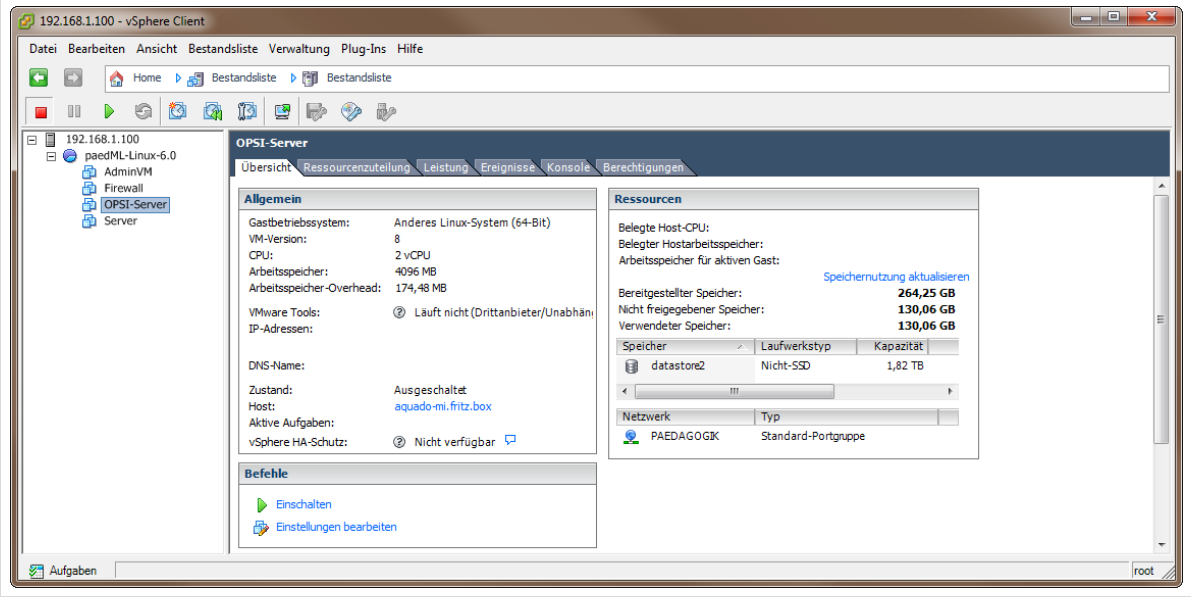


Abb. 129: Übersichtsseite der VM „opsi-Server“ im Auslieferungszustand

Übersichtsseite VM „AdminVM“

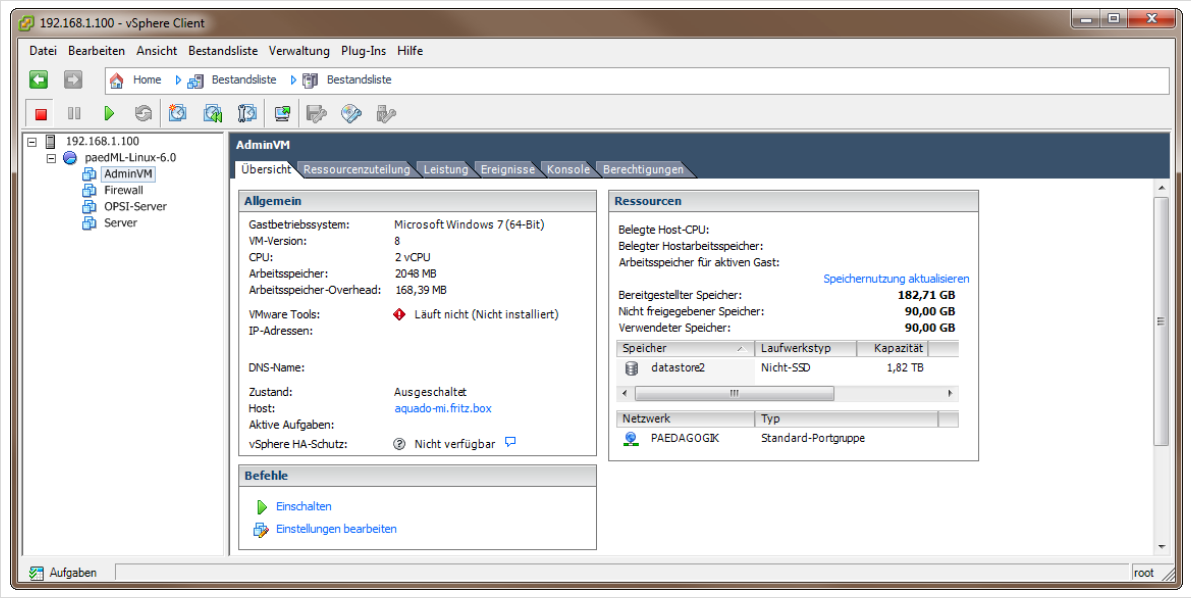


Abb. 130: Übersichtsseite der virtuellen Maschine „AdminVM“ im Auslieferungszustand.

5. Basiskonfiguration der virtuellen Maschinen

Es erfolgt die Basiskonfiguration der drei importierten Maschinen „*Firewall*“, „*Server*“ und „*opsi-Server*“, die Maschine „*AdminVM*“ erfordert ein gesondertes Vorgehen, dies wird in Kapitel 6 ab Seite 104 beschrieben.

Schalten Sie die virtuellen Maschinen immer in der angegebenen Reihenfolge ein!

Warten Sie dabei stets mit dem Start der nächsten Maschine, bis die vorherige vollständig hochgefahren ist!

Die virtuellen Server „*Firewall*“, „*Server*“ und „*opsi-Server*“ müssen nun in der folgenden Reihenfolge eingeschaltet werden.

1. *Firewall*
1. *Server*
2. *opsi-Server*

Markieren Sie dazu im *vSphere-Client* jeweils die entsprechende Maschine mit der Maus und klicken Sie auf den Button „*VM einschalten*“ (Symbol in rotem Kreis)

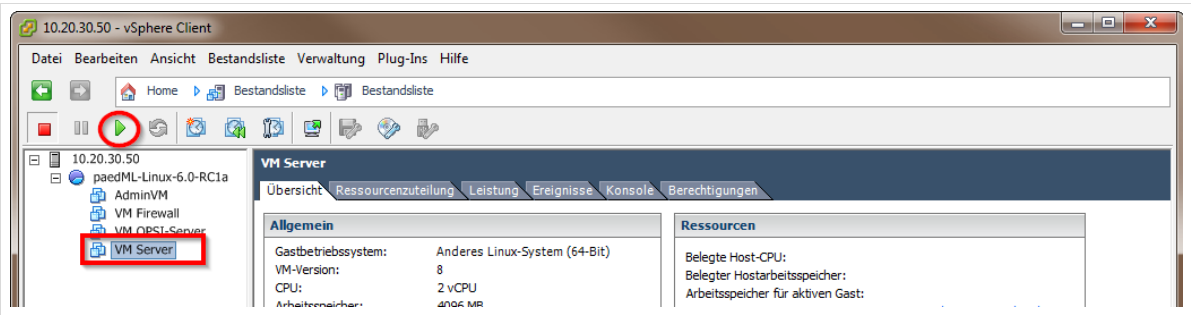


Abb. 131: Einschalten einer virtuellen Maschine über den vSphere-Client

Die **Passwörter** für alle zentralen Benutzerkonten wie *root* oder *Administrator* (Domänen-Administrator) sind initial auf den Wert „*paedmllinux*“ gesetzt.

5.1 Basiskonfiguration der VM „Firewall“

Die externe Netzwerkkarte der Firewall (Netz „*INTERNET*“) ist im Auslieferungszustand auf den Bezug von dynamischen IP-Adressen konfiguriert. Falls die Firewall über das externe Interface keine IP-Adresse per DHCP zugewiesen bekommt, muss das externe Netzwerkinterface zwingend auf eine statische IP-Adresse umgestellt werden.

Falls im Netz „*INTERNET*“ bereits ein DHCP-Service aktiv ist (z.B. auf einem DSL-Router), ist die Umstellung auf eine statische IP-Adresse zwar nicht zwingend erforderlich. Das Arbeiten mit statischen IP-Adressen (und eventuell das Deaktivieren eines DHCP-Servers) im Netz „*INTERNET*“ kann unter

Umständen zu einer stabileren Netzwerkkonfiguration führen. Die Fehlersuche bei Netzwerkproblemen wird hierdurch ebenfalls erleichtert.

Solange es für die Verwendung von DHCP im Netz „*INTERNET*“ keine zwingenden Gründe gibt, wird die Verwendung von statischen IP-Adressen empfohlen.

Veränderungen an den Einstellungen der Firewall dürfen nur per Browser über die Web-Schnittstelle („*WebGUI*“) vorgenommen werden.

Die über die Textkonsole angebotenen Funktionen zur Netzkonfiguration dürfen nicht genutzt werden!

5.1.1 IP-Konfiguration der externen Netzwerkkarte

Login auf der WebGUI der Firewall

Öffnen Sie im Browser die WebGUI der Firewall unter http://firewall.paedml-linux.lokal und melden Sie sich als Benutzer „*admin*“ an (initiales Passwort ist „*paedmllinux*“).

Abb. 132: Login-Maske der Firewall

Umstellen der externen Netzwerkkarte auf statische IP-Adresse

Navigieren Sie zum Punkt „*Interfaces* | *INTERNET*“ um die Einstellungen der externen Netzwerkkarte zu ändern.

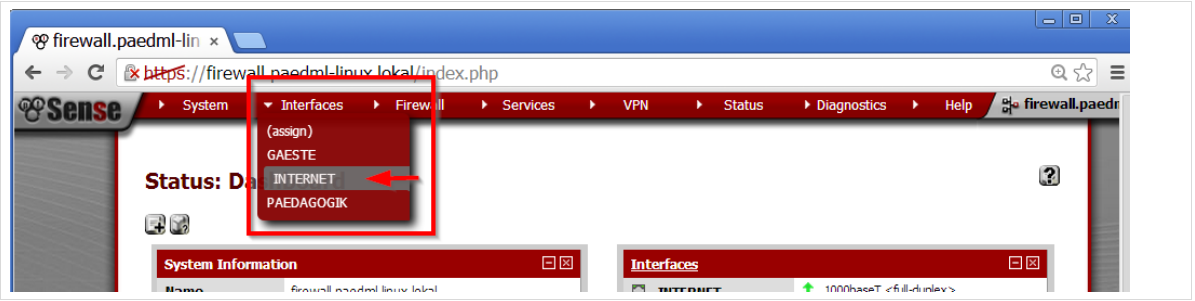


Abb. 133: Navigation zu den Einstellungen der externen Netzwerkkarte

Führen Sie im folgenden Fenster folgende Änderungen durch:

- Ändern Sie die Einstellung „*IPv4 Configuration Type*“ auf „*Static IPv4*“.
- Tragen Sie im Feld „*IPv4 address*“ die statische IP-Adresse des externen Interfaces sowie den Netzbereich ein. **Die Adresse und die Subnetzmaske sind abhängig von der lokal gegebenen Netzwerkkonfiguration und muss an diese angepasst werden!**
- Wählen Sie im Feld „*Gateway*“ die IP-Adresse des Gateways für den Internetzugang (z.B. die interne IP-Adresse ihres DSL-Routers) aus, falls das Gateway der Firewall schon bekannt ist. Im Regelfall ist dieses Gateway der Firewall aber noch nicht bekannt und muss zunächst durch Klick auf „*add a new one*“ angelegt werden.

firewall.paedml-lin
https://firewall.paedml-linux.lokal/interfaces.php?if=wan
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Interfaces: INTERNET
General configuration
Enable
Enable Interface
Description
INTERNET
Enter a description (name) for the interface here.
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC address
Insert my local MAC address
This field can be used to modify ("spoof") the MAC address of this interface
(may be required with some cable connections)
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank
MTU
If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.
Speed and duplex
Advanced
- Show advanced option
Static IPv4 configuration
IPv4 address
192.168.1.15
Gateway
None
- or add a new one.
If this interface is an Internet connection, select an existing Gateway from the list or add one using the link above
Private networks

Abb. 134: Einstellen der externen IP-Adresse

Nach Klick auf „*add a new one*“ kann das Gateway in der Firewall angelegt werden:

- Setzen Sie den Haken bei „*Default gateway*“
- Vergeben Sie unter „*Gateway Name*“ einen Namen für das Gateway oder übernehmen Sie die Voreinstellung „*INTERNETGW*“
- Tragen Sie unter „*Gateway IPv4*“ die LAN-seitige IP-Adresse des Gateways ein.
- Vergeben Sie unter „*Description*“ eine Beschreibung für das Gateway (Freitextfeld).
- Speichern Sie die Änderungen durch Klick auf „*Save Gateway*“.

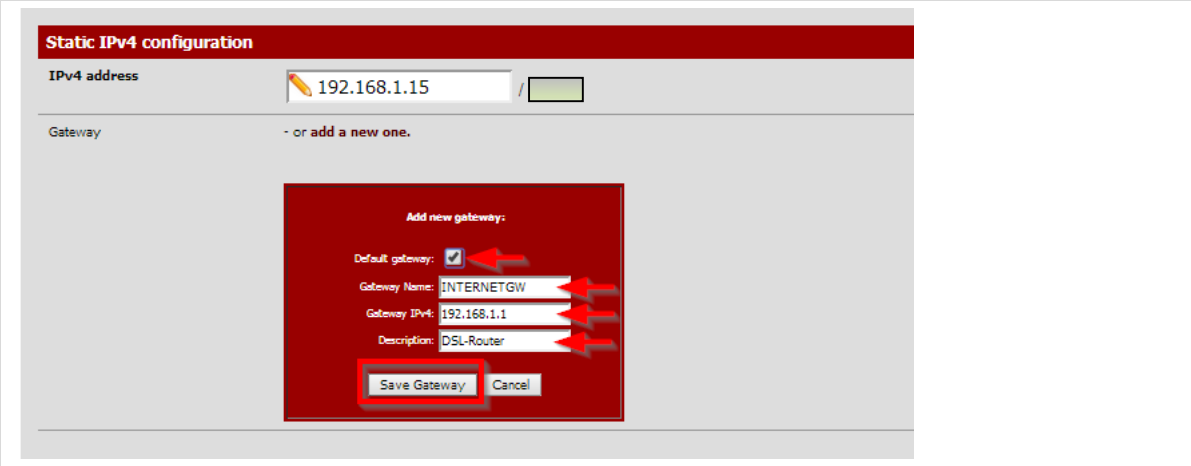


Abb. 135: Anlegen eines neuen Gateways

Nun kann das eben angelegte Gateway ausgewählt werden. Speichern Sie mit Klick auf „*Save*“.

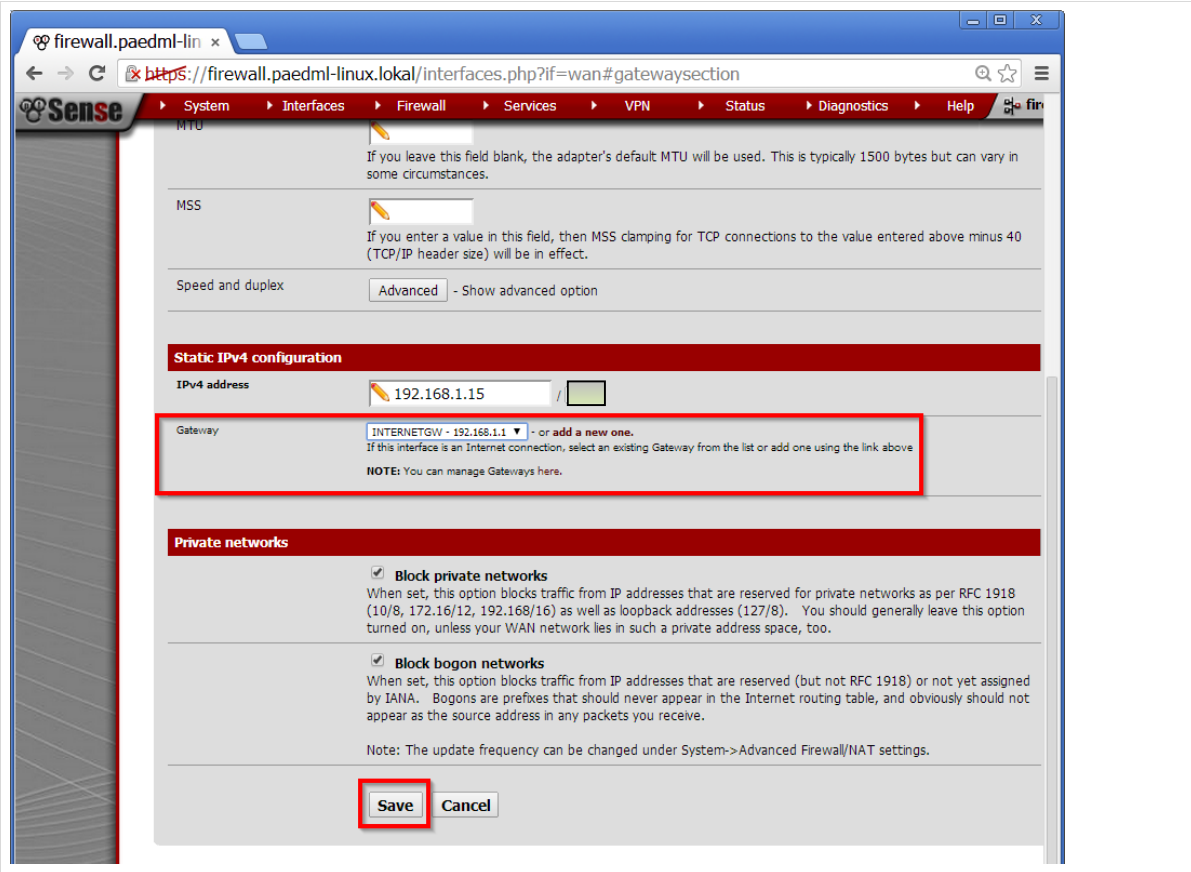

firewall.paedml-lin
https://firewall.paedml-linux.lokal/interfaces.php?if=wan#gatewaysection
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
MTU
If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.
Speed and duplex
Advanced
- Show advanced option
Static IPv4 configuration
IPv4 address
192.168.1.15
Gateway
INTERNETGW - 192.168.1.1
- or add a new one.
If this interface is an Internet connection, select an existing Gateway from the list or add one using the link above
NOTE: You can manage Gateways here.
Private networks
Block private networks
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.
Block bogon networks
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets you receive.
Note: The update frequency can be changed under System->Advanced Firewall/NAT settings.
Save
Cancel

Abb. 136: Eintragen des Gateways

Die neue Konfiguration muss anschließend übernommen werden. Dies geschieht über einen Klick auf „*Apply changes*“.

Abb. 137: Übernahme der Änderungen in den laufenden Betrieb

Einstellen der DNS-Server

Wird die IP-Adresse der externen Netzwerkkarte manuell eingetragen, dann müssen die zu verwendenden DNS-Server ebenfalls manuell eingestellt werden. Navigieren Sie dazu auf „*System* | *General Setup*“.

Abb. 138: Navigation zu den Grundeinstellungen der Firewall

Tragen Sie nun die IP-Adressen der DNS-Server in die entsprechenden Felder ein. Hierfür gibt es – je nach Art der Internetverbindung – verschiedene Alternativen:

- Die DNS-Server werden von ihrem Internetanbieter vorgegeben. Für BelWü-Kunden sind dies zum Beispiel *129.143.2.1* und *129.143.2.4*.
- Falls Sie den DNS-Server nicht kennen, können Sie versuchen, die IP-Adresse ihres Internetrouters einzutragen. Dies setzt allerdings voraus, dass Ihr Internetrouter seinerseits die DNS-Anfragen korrekt verarbeitet, was häufig bei Routern der Consumer-Klasse nicht zuverlässig funktioniert.
- Sie tragen die IP-Adresse von frei verfügbaren DNS-Servern ein (z.B. die DNS-Server von Google *8.8.8.8* oder *8.8.4.4*).

Jedem DNS-Server muss das im Menü „*Interfaces Internet*“ definierte Gateway zugewiesen werden.

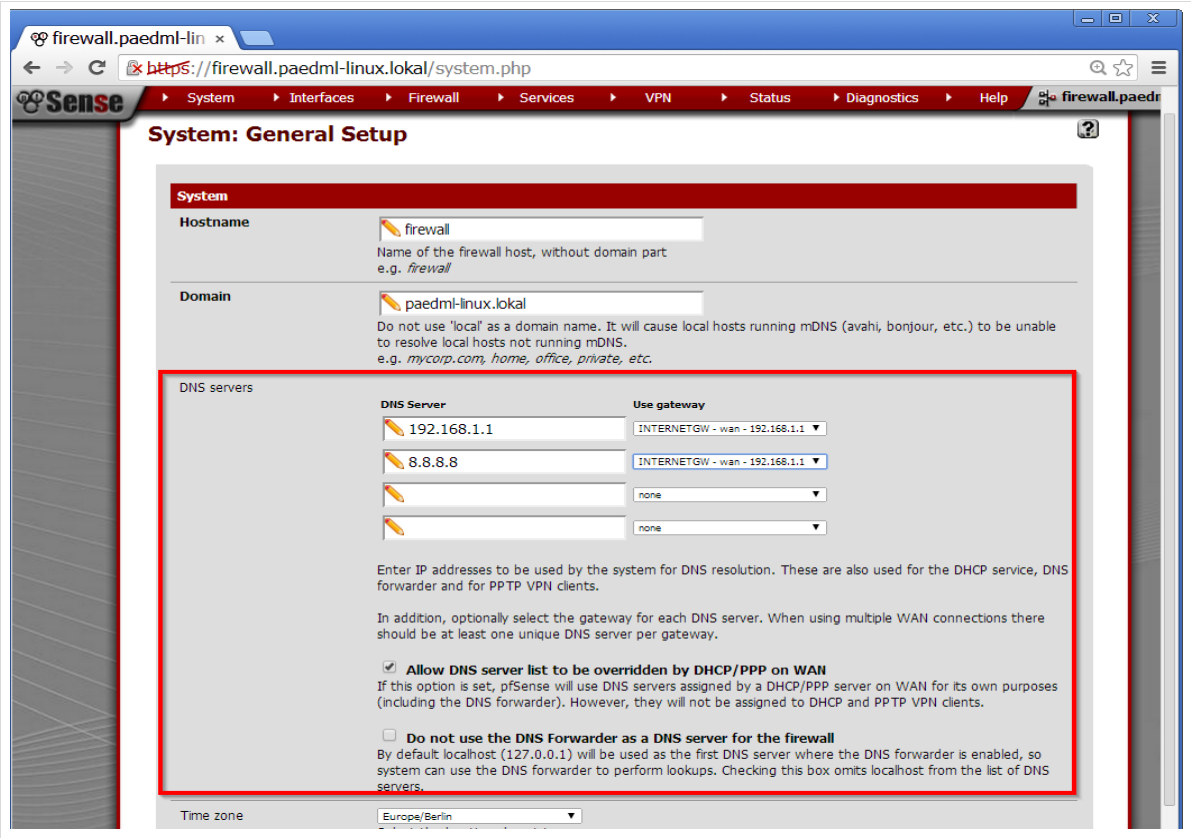

firewall.paedml-lin
https://firewall.paedml-linux.lokal/system.php
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
System: General Setup
Hostname
firewall
Name of the firewall host, without domain part
e.g. firewall
Domain
paedml-linux.lokal
Do not use 'local' as a domain name. It will cause local hosts running mDNS (avahi, bonjour, etc.) to be unable to resolve local hosts not running mDNS.
e.g. mycorp.com, home, office, private, etc.
DNS servers
DNS Server
Use gateway
192.168.1.1
8.8.8.8
INTERNETGW - wan - 192.168.1.1
none
Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS forwarder and for PPTP VPN clients.
In addition, optionally select the gateway for each DNS server. When using multiple WAN connections there should be at least one unique DNS server per gateway.
Allow DNS server list to be overridden by DHCP/PPP on WAN
If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS forwarder). However, they will not be assigned to DHCP and PPTP VPN clients.
Do not use the DNS Forwarder as a DNS server for the firewall
By default localhost (127.0.0.1) will be used as the first DNS server where the DNS forwarder is enabled, so system can use the DNS forwarder to perform lookups. Checking this box omits localhost from the list of DNS servers.
Time zone
Europe/Berlin

Abb. 139: Eintragen der DNS-Server

Die Einrichtung der Firewall ist hiermit abgeschlossen. Sie können die Internetverbindung testen, in dem Sie über das *pfSense*-Menü „*Diagnostics* | *Ping*“ eine Internetseite pingen.

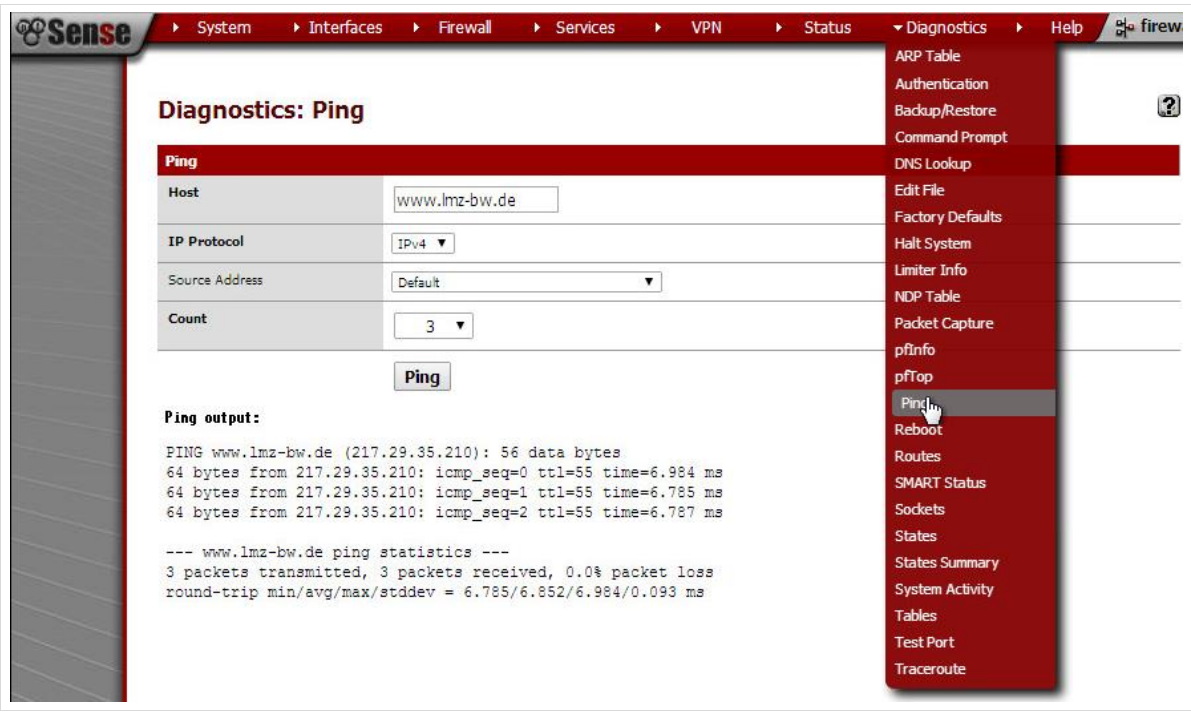


Abb. 140: Erfolgreicher Ping-Versuch auf www.lmz-bw.de

5.2 Basiskonfiguration der VM „Server“

Auf der VM „*Server*“ muss nach dem Import die **Systemindividualisierung** durchgeführt werden.

Im Auslieferungszustand sind alle *paedML Linux*-Installationen zunächst vollständig identisch, so sind alle Passwörter auf „*paedmllinux*“ gesetzt.

Für einen sicheren Betrieb muss die *paedML Linux*-Installation individualisiert werden, hierbei werden unter anderem alle Passwörter geändert, die SSH-Schlüssel und SSL-Zertifikate neu generiert sowie weitere sicherheitsrelevante Konfigurationen ausgetauscht.

Bei der Individualisierung werden außerdem Lizenzinformationen, die für den Betrieb der *paedML Linux* notwendig sind, in das System übernommen.

5.2.1 Durchführen der Systemindividualisierung

Die Systemindividualisierung kann nur bei bestehender Internetverbindung durchgeführt werden!

Um Ihren Server einzurichten, benötigen Sie Zugangsdaten, die Sie nach der Bestellung einer paedML Linux ab Version 6.0 erhalten.

1. Melden Sie sich an der Server-Konsole als Benutzer *root* an.
2. Vergewissern Sie sich, dass die virtuellen Maschinen „*opsi-Server*“ und „*Firewall*“ ebenfalls eingeschaltet und per Netzwerk vom Server aus erreichbar sind:
   2.1. Pingen der VM „*opsi-Server*“: `#ping backup.paedml-linux.lokal`
   2.2. Pingen der VM „*Firewall*“: `#ping firewall.paedml-linux.lokal`
3. Vergewissern Sie sich, dass der Server eine Verbindung zum Internet hat: `#ping www.lmz-bw.de`
4. Rufen Sie das Skript für den Individualisierungs-Prozess mit dem Befehl `#lmz-initial-setup` auf:

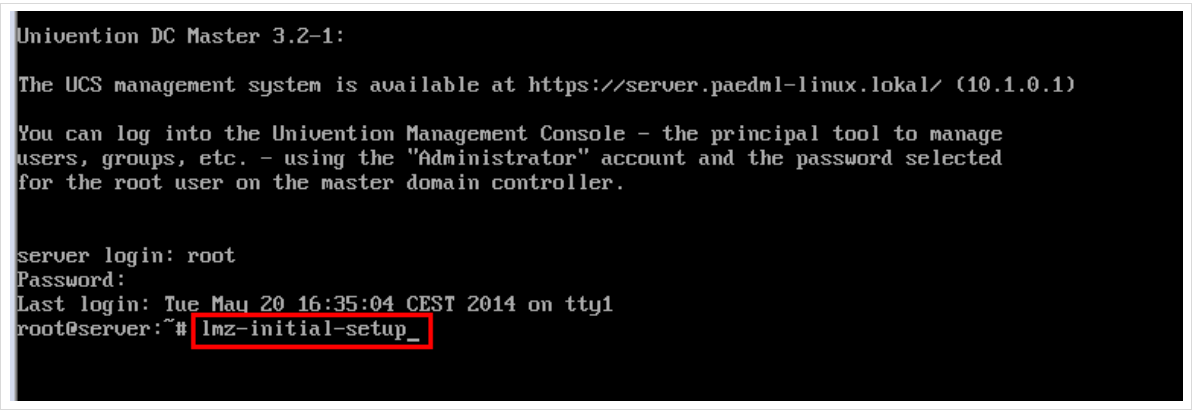

Univention DC Master 3.2-1:
The UCS management system is available at https://server.paedml-linux.lokal/ (10.1.0.1)
You can log into the Univention Management Console - the principal tool to manage
users, groups, etc. - using the "Administrator" account and the password selected
for the root user on the master domain controller.
server login: root
Password:
Last login: Tue May 20 16:35:04 CEST 2014 on tty1
root@server:~# lmz-initial-setup_

Abb. 141: Start der Systemindividualisierung auf der Konsole des Servers

Das System fragt Sie zunächst nach Ihrer *paedML Linux*-Installationsnummer, die Sie vom LMZ erhalten, und dem dazugehörigen Passwort. Geben Sie diese beiden Werte ein:

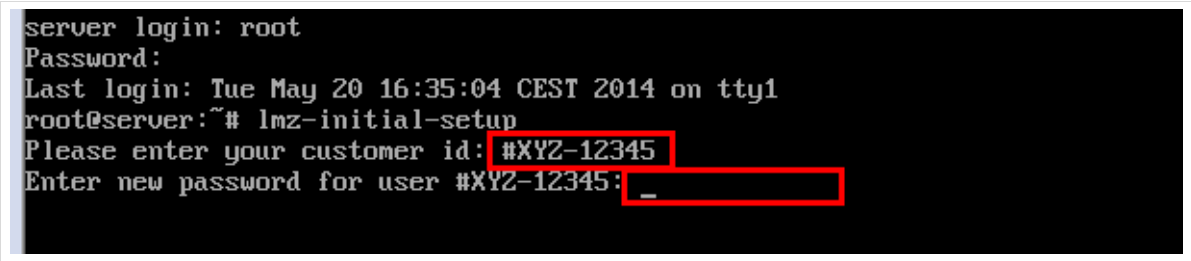

server login: root
Password:
Last login: Tue May 20 16:35:04 CEST 2014 on tty1
root@server:~# lmz-initial-setup
Please enter your customer id: #XYZ-12345
Enter new password for user #XYZ-12345:

Abb. 142: Abfrage der Installationsnummer

Anschließend werden Sie nach den gewünschten neuen Passwörtern für zentrale Benutzerkonten) gefragt. Tragen Sie dort ein **selbst gewähltes Passwort** ein. Dieses Passwort wird für die folgenden Benutzer gesetzt:

- *root* (Server, opsi-Server)
- *Administrator* (Domänen-Administrator, *pfSense*-Administrator, opsi-Administrator)
- *domadmin* (Konto für die Clientaufnahme)
- *netzwerkberater* (administratives Benutzerkonto mit eingeschränkten Rechten)

root@server:~# lmz-initial-setup
Please enter your customer id:
Enter new password for user
Enter new password for user Administrator/domadmin/netzwerkberater/root:
Confirm password:

Abb. 143: Vergabe eines neuen Passwortes für zentrale Benutzerkonten

Nun beginnt der Individualisierungsprozess. Dieser kann einige Minuten dauern, die Ausgabe kann auf der Konsole beobachtet werden:

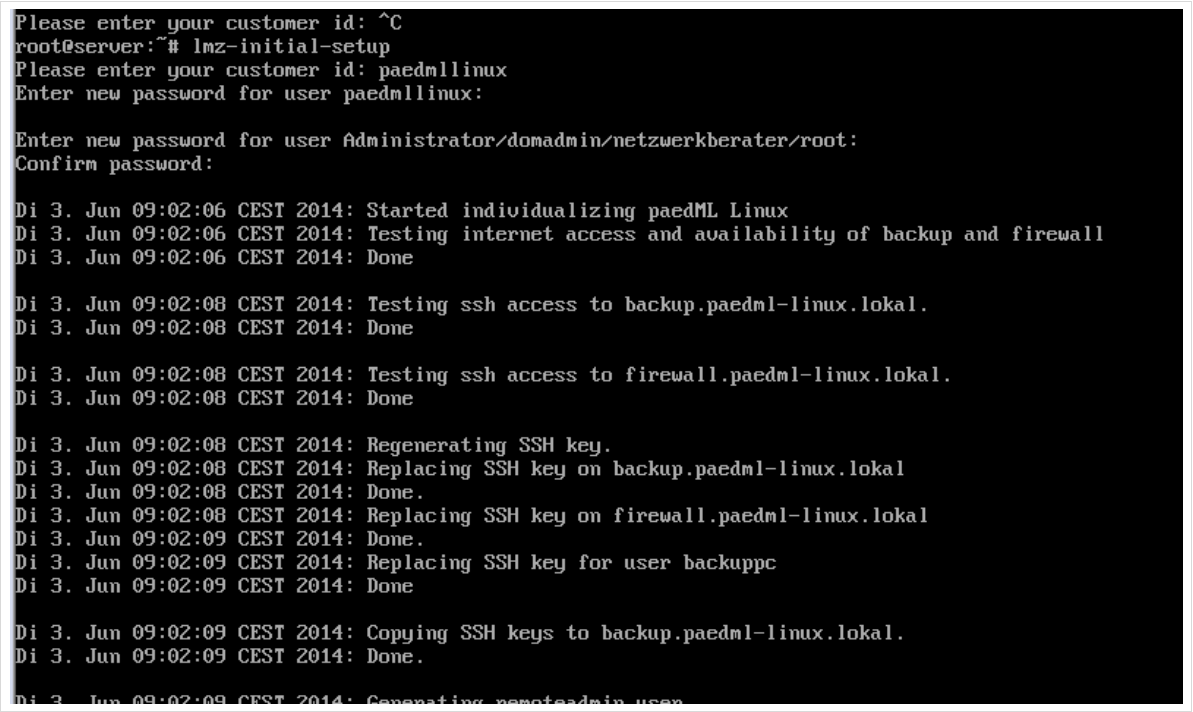

Please enter your customer id: ^C
root@server:~# lmz-initial-setup
Please enter your customer id: paedmllinux
Enter new password for user paedmllinux:
Enter new password for user Administrator/domadmin/netzwerkberater/root:
Confirm password:
Di 3. Jun 09:02:06 CEST 2014: Started individualizing paedML Linux
Di 3. Jun 09:02:06 CEST 2014: Testing internet access and availability of backup and firewall
Di 3. Jun 09:02:06 CEST 2014: Done
Di 3. Jun 09:02:08 CEST 2014: Testing ssh access to backup.paedml-linux.lokal.
Di 3. Jun 09:02:08 CEST 2014: Done
Di 3. Jun 09:02:08 CEST 2014: Testing ssh access to firewall.paedml-linux.lokal.
Di 3. Jun 09:02:08 CEST 2014: Done
Di 3. Jun 09:02:08 CEST 2014: Regenerating SSH key.
Di 3. Jun 09:02:08 CEST 2014: Replacing SSH key on backup.paedml-linux.lokal
Di 3. Jun 09:02:08 CEST 2014: Done.
Di 3. Jun 09:02:08 CEST 2014: Replacing SSH key on firewall.paedml-linux.lokal
Di 3. Jun 09:02:09 CEST 2014: Done.
Di 3. Jun 09:02:09 CEST 2014: Replacing SSH key for user backuppc
Di 3. Jun 09:02:09 CEST 2014: Done
Di 3. Jun 09:02:09 CEST 2014: Copying SSH keys to backup.paedml-linux.lokal.
Di 3. Jun 09:02:09 CEST 2014: Done.

Abb. 144: Die Systemindividualisierung wird durchgeführt

Erfolgreicher Durchlauf

Läuft das Skript erfolgreich durch, so sollten Sie die Meldung „*Finished individualizing paedML*“ sehen. Drücken Sie Enter, daraufhin werden alle *paedML Linux* Server neu gestartet.

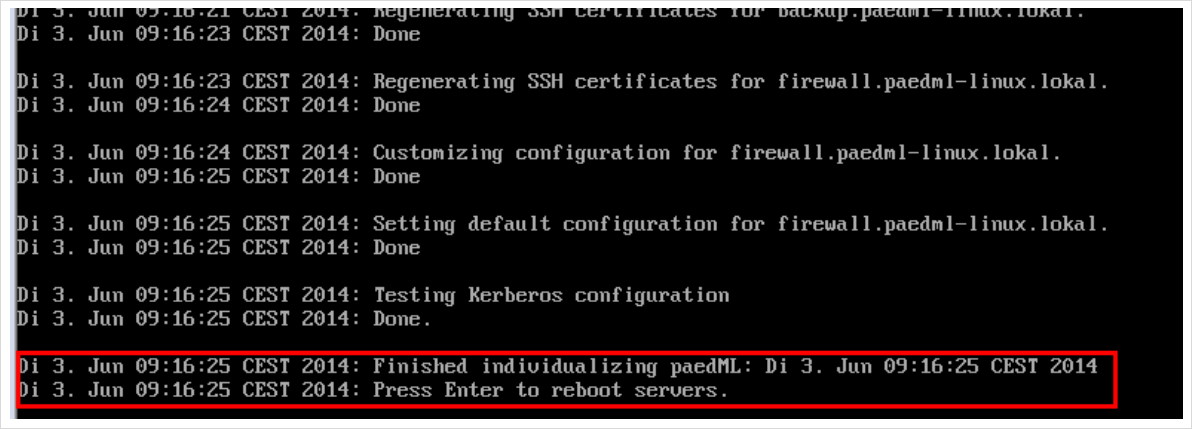

Di 3. Jun 09:16:23 CEST 2014: Done
Di 3. Jun 09:16:23 CEST 2014: Regenerating SSH certificates for firewall.paedml-linux.lokal.
Di 3. Jun 09:16:24 CEST 2014: Done
Di 3. Jun 09:16:24 CEST 2014: Customizing configuration for firewall.paedml-linux.lokal.
Di 3. Jun 09:16:25 CEST 2014: Done
Di 3. Jun 09:16:25 CEST 2014: Setting default configuration for firewall.paedml-linux.lokal.
Di 3. Jun 09:16:25 CEST 2014: Done
Di 3. Jun 09:16:25 CEST 2014: Testing Kerberos configuration
Di 3. Jun 09:16:25 CEST 2014: Done.
Di 3. Jun 09:16:25 CEST 2014: Finished individualizing paedML: Di 3. Jun 09:16:25 CEST 2014
Di 3. Jun 09:16:25 CEST 2014: Press Enter to reboot servers.

Abb. 145: Erfolgreicher Abschluss des Individualisierungsprozesses

Mögliche Fehlerquellen

Falls keine Internetverbindung besteht oder die anderen Maschinen per Netzwerk nicht erreichbar sind, so bricht das Skript mit einer der folgenden Meldungen ab:

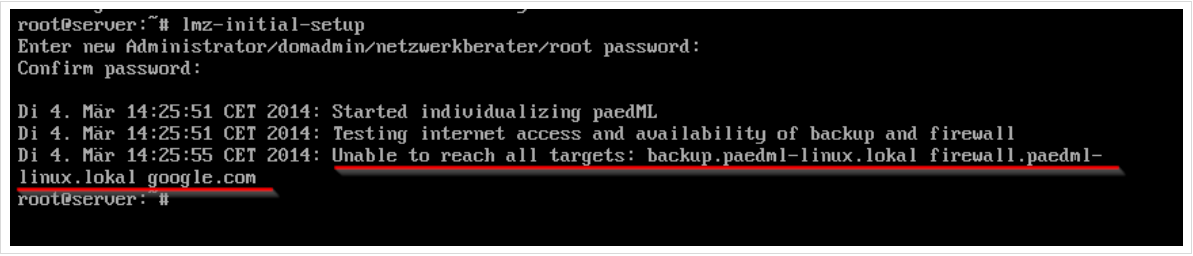

root@server:~# lmz-initial-setup
Enter new Administrator/domadmin/netzwerkberater/root password:
Confirm password:
Di 4. Mär 14:25:51 CET 2014: Started individualizing paedML
Di 4. Mär 14:25:51 CET 2014: Testing internet access and availability of backup and firewall
Di 4. Mär 14:25:55 CET 2014: Unable to reach all targets: backup.paedml-linux.lokal firewall.paedml-linux.lokal google.com
root@server: #

Abb. 146: Abbruch des Individualisierungsprozesses bei fehlender Internetverbindung

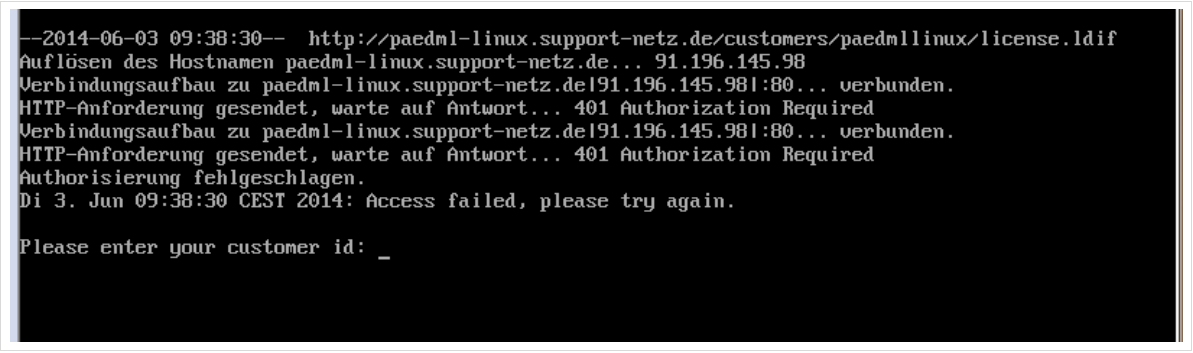

--2014-06-03 09:38:30-- http://paedml-linux.support-netz.de/customers/paedmllinux/license.ldif
Auflösen des Hostnamen paedml-linux.support-netz.de... 91.196.145.98
Verbindungsaufbau zu paedml-linux.support-netz.de|91.196.145.98|:80... verbunden.
HTTP-Anforderung gesendet, warte auf Antwort... 401 Authorization Required
Verbindungsaufbau zu paedml-linux.support-netz.de|91.196.145.98|:80... verbunden.
HTTP-Anforderung gesendet, warte auf Antwort... 401 Authorization Required
Authorisierung fehlgeschlagen.
Di 3. Jun 09:38:30 CEST 2014: Access failed, please try again.
Please enter your customer id: _

Abb. 147: Abbruch des Individualisierungsprozesses

Brechen Sie das ggf. noch laufende Skript mit Strg+C ab. Stellen Sie daraufhin sicher, dass

- alle virtuellen Maschinen eingeschaltet sind,
- die Konfiguration der virtuellen Netzwerke korrekt durchgeführt wurde,
- alle Maschinen sich untereinander mit dem DNS-Namen pingen können,
- vom Server aus eine Internetverbindung besteht.

Starten Sie den Individualisierungsvorgang nach der Behebung möglicher Fehler erneut.

5.2.2 Optional: Ändern des Passwortes von „domadmin“

Dieser Schritt ist notwendig, wenn Sie die Domänenaufnahme von Geräten durch Personen, die nicht Dienstleister oder Netzwerkberater sind, durchführen lassen.

Das Kennwort des Accounts *domadmin* sollte in diesem Fall von den Kennwörtern der Benutzer *root, Administrator* und netzwerkberaterabweichen!

Da bei der Systemindividualisierung mit `#lmz-initial-setup` alle Kennwörter auf den gleichen Wert gesetzt werden, ist es gegebenenfalls notwendig, das Kennwort des Benutzers *domadmin* zu ändern.

Hier wird nur die Passwortänderung für den Benutzer *domadmin* erklärt.

Im Administratorhandbuch ist die Änderung der Kennwörter administrativer Benutzer beschrieben.

Zum Ändern des domadmin-Passworts gehen Sie wie folgt vor:

1. Melden Sie sich als Benutzer *root* auf der Konsole des Servers an.
2. Rufen Sie das Kommando `#lmz-initial-setup` --domadmin auf.
3. Geben Sie auf Nachfrage das neue Passwort für den Benutzer *domadmin* ein.
4. Geben Sie auf Nachfrage das neue Passwort ein zweites Mal ein.
5. Daraufhin wird das Passwort für den Benutzer *domadmin* geändert. Nach Ablauf des Skripts drücken Sie auf ENTER.
6. In der Regel ist danach – im Gegensatz zur vollständigen Systemindividualisierung – kein Neustart der Server mehr nötig.
7. Melden Sie sich von der Konsole mit dem Befehl `#exit` ab.

5.2.3 Aktualisieren des Basissystems der VM „Server“

Zu Beginn müssen Sie das Basissystem einmalig manuell auf den aktuellen Softwarestand bringen. Spätere Updates werden dann automatisch ausgeführt.

Loggen Sie sich als Benutzer „*root*“ auf der Konsole der VM „*Server*“ ein. Starten Sie den Vorgang mit dem Befehl

```
#univention-upgrade
```

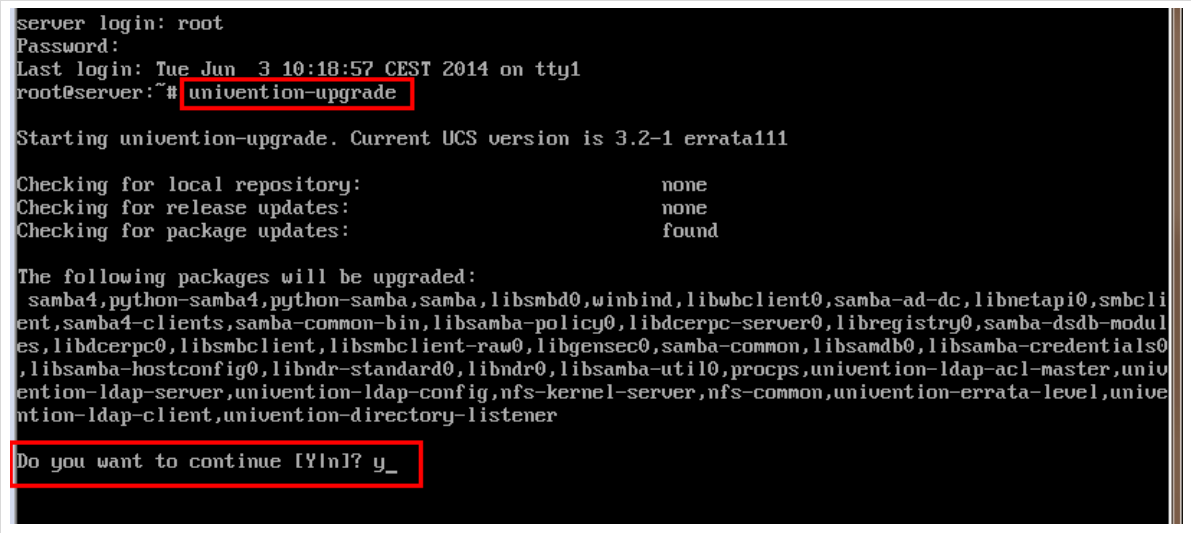


Abb. 148: Upgrade des Servers und Sicherheitsabfrage

Es wird eine Liste von aktualisierbaren Paketen angezeigt. Es folgt nochmals eine Abfrage:
„*Do you want to continue [Y|n]?*“

Bestätigen Sie diese Abfrage durch Eingabe von y und Enter. Darauf werden die aktuellen Updates eingespielt, Dieser Vorgang kann – je nach Größe der Updates und Geschwindigkeit der Internetverbindung – einige Zeit in Anspruch nehmen. Am Ende des Updatevorgangs erscheint wieder der Cursor.

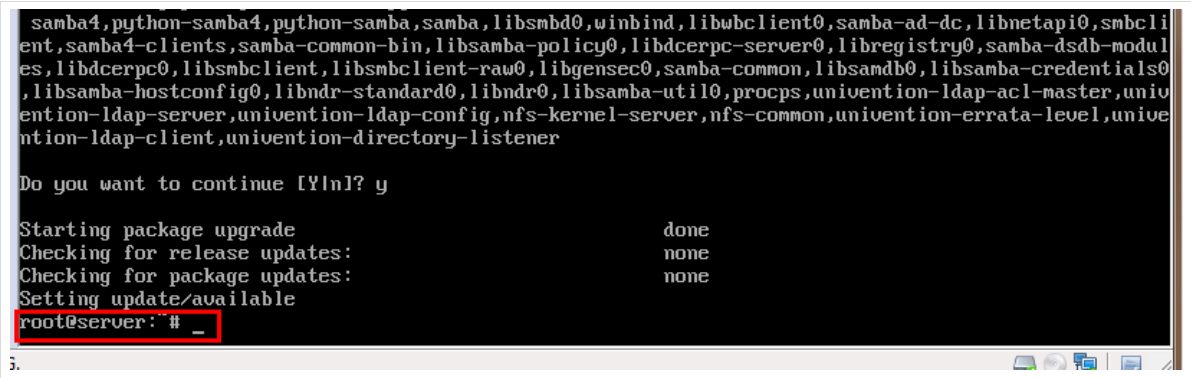


Abb. 149: Der Updatevorgang wurde erfolgreich ausgeführt.

Starten Sie nach dem Update den Server neu, damit alle geänderten Systemdienste neu gestartet werden können.

5.3 Basiskonfiguration der VM „opsi-Server“

Hinweis: Die VM „*opsi-Server*“ wird auf der Konsole unter dem Namen als „*backup*“ angezeigt.

5.3.1 Aktualisieren des Basissystems der VM „opsi-Server“

Zu Beginn müssen Sie das Basissystem einmalig manuell auf den aktuellen Softwarestand bringen. Spätere Updates werden dann automatisch ausgeführt.

Loggen Sie sich als Benutzer „*root*“ auf der Konsole der VM „*opsi-Server*“ ein.

Starten Sie den Updatevorgang mit dem Befehl

```
#univention-upgrade
```

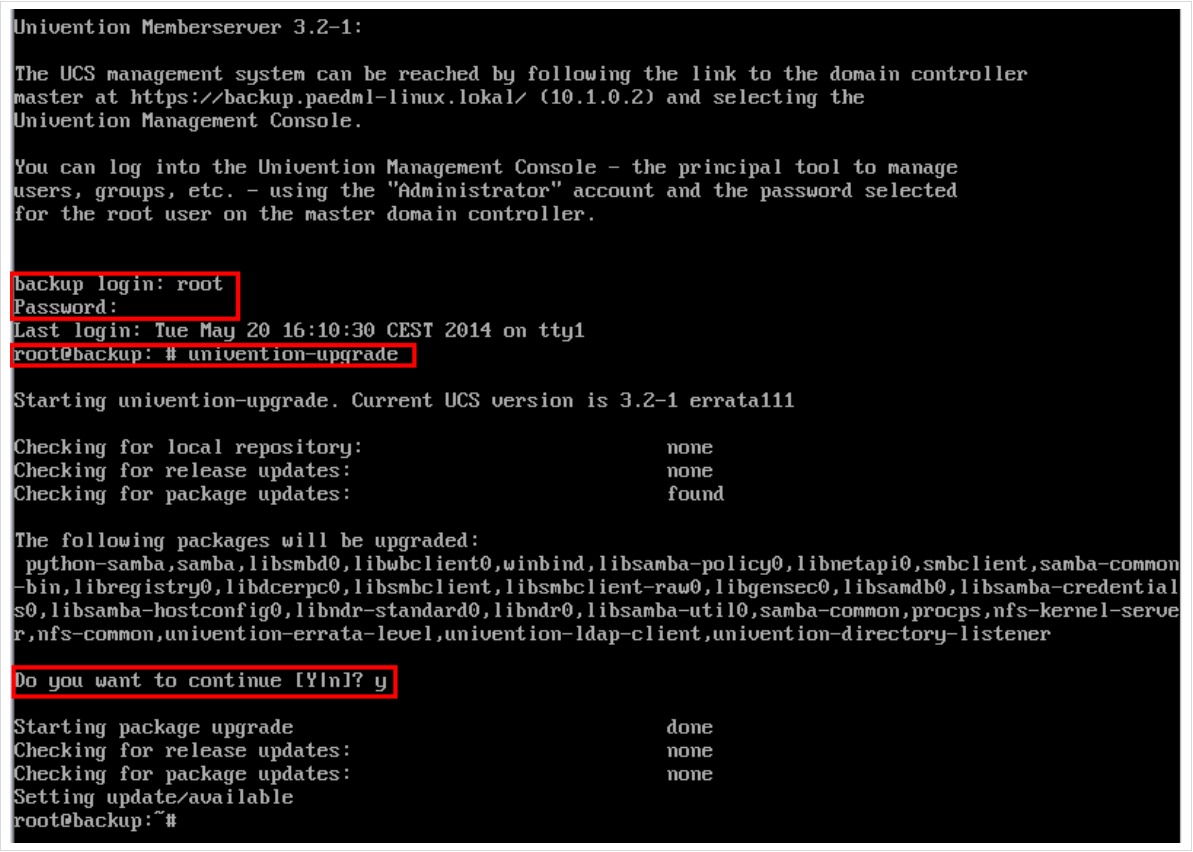

Univention Memberserver 3.2-1:
The UCS management system can be reached by following the link to the domain controller
master at https://backup.paedml-linux.lokal/ (10.1.0.2) and selecting the
Univention Management Console.
You can log into the Univention Management Console - the principal tool to manage
users, groups, etc. - using the "Administrator" account and the password selected
for the root user on the master domain controller.
backup login: root
Password:
Last login: Tue May 20 16:10:30 CEST 2014 on tty1
root@backup: # univention-upgrade
Starting univention-upgrade. Current UCS version is 3.2-1 errata111
Checking for local repository: none
Checking for release updates: none
Checking for package updates: found
The following packages will be upgraded:
python-samba,samba,libsmbd0,libwbclient0,winbind,libsamba-policy0,libnetapi0,smbclient,samba-common
-bin,libregistry0,libdcerpc0,libsmbclient,libsmbclient-raw0,libgensec0,libsamdb0,libsamba-credential
s0,libsamba-hostconfig0,libndr-standard0,libndr0,libsamba-util0,samba-common,procps,nfs-kernel-serve
r,nfs-common,univention-errata-level,univention-ldap-client,univention-directory-listener
Do you want to continue [Y|n]? y
Starting package upgrade done
Checking for release updates: none
Checking for package updates: none
Setting update/available
root@backup:~#

Abb. 150: Update der VM „opsi-Server“

Es wird eine Liste von aktualisierbaren Paketen angezeigt. Es folgt nochmals eine Abfrage *„Do you want to continue [Y|n]?“*

Bestätigen Sie diese Abfrage durch Eingabe von y und Enter. Darauf werden die aktuellen Updates eingespielt., Dieser Vorgang kann – je nach Größe der Updates und Geschwindigkeit der Internetverbindung – einige Zeit in Anspruch nehmen. Am Ende des Updatevorgangs erscheint wieder der Cursor.

5.3.2 Aktualisieren der opsi-Produkte

Auf der VM „*opsi-Server*“ müssen im nächsten Schritt alle *opsi*-Produkte auf den neusten Stand gebracht werden

Melden Sie sich auf der Textkonsole der VM „*opsi-Server*“ als Benutzer „*root*“ an. Sie lösen den Updatevorgang mit dem folgenden Befehl aus:

```
#opsi-product-updater -vv
```

Durch Eingabe dieses Befehls werden die *opsi* -Produkte auf den neusten Stand gebracht. Dieser Vorgang kann – abhängig von Menge und Größe der Updates und der Internetbandbreite – einige Zeit (auch mehrere Stunden) in Anspruch nehmen.

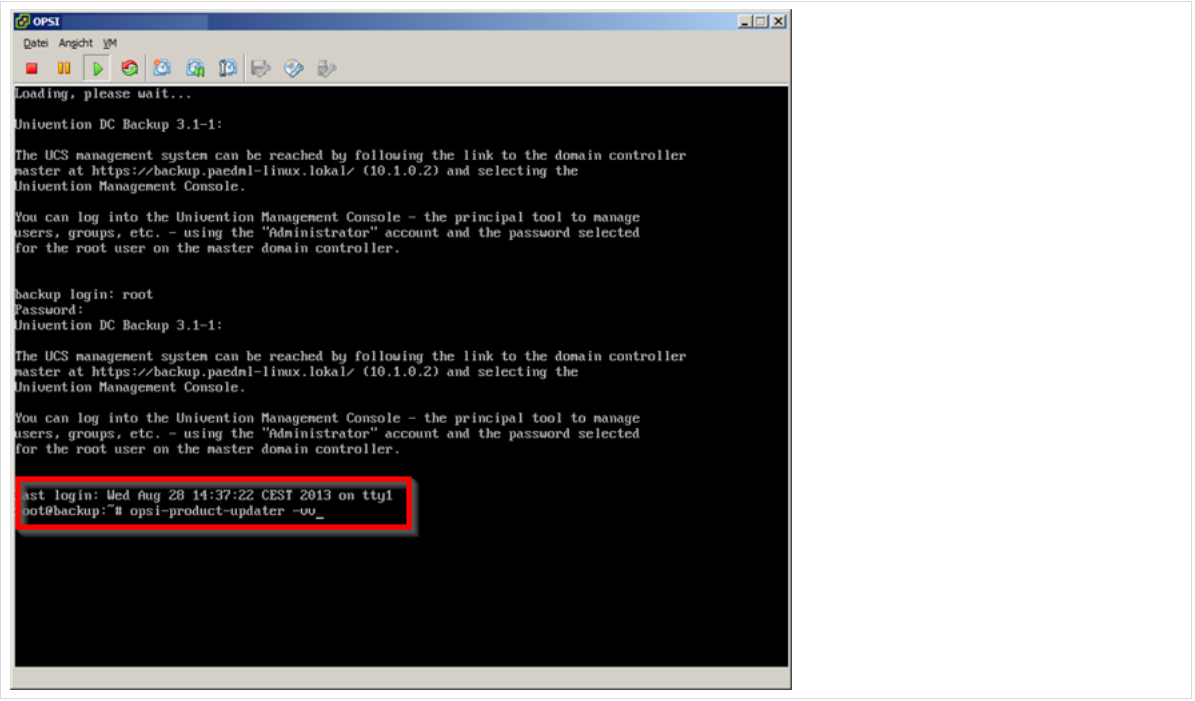

OPSI
Datei Ansicht VM
Loading, please wait...
Univention DC Backup 3.1-1:
The UCS management system can be reached by following the link to the domain controller master at https://backup.paedml-linux.lokal/ (10.1.0.2) and selecting the Univention Management Console.
You can log into the Univention Management Console - the principal tool to manage users, groups, etc. - using the "Administrator" account and the password selected for the root user on the master domain controller.
backup login: root
Password:
Univention DC Backup 3.1-1:
The UCS management system can be reached by following the link to the domain controller master at https://backup.paedml-linux.lokal/ (10.1.0.2) and selecting the Univention Management Console.
You can log into the Univention Management Console - the principal tool to manage users, groups, etc. - using the "Administrator" account and the password selected for the root user on the master domain controller.
ast login: Wed Aug 28 14:37:22 CEST 2013 on tty1
oot@backup:~# opsi-product-updater -vv_

Abb. 151: Update aller opsi-*Produkte auf der Konsole der VM „*opsi-*Server“*

Starten Sie nach dem Update den opsi-Server neu, damit alle geänderten Systemdienste neu gestartet werden können.

5.4 Updaten der Firewall

Die in der *paedML Linux* verwendete Firewall-Lösung „*pfSense*“ besitzt einen einfachen Updatemechanismus, mit dem die Software der Firewall (in *pfSense*-Nomenklatur „Firmware“) stets aktuell gehalten werden kann.

Zu Beginn der *paedML Linux*-Installation sollte die Firmware der *pfSense* manuell auf den aktuellen Stand gebracht werden.

Das Support-Netz pflegt ein in der *pfSense* eingetragenes Repository, in dem Updates für die Firewall vorgehalten werden.

Das System ist so konfiguriert, dass es automatisch prüft, ob in diesem Repository Aktualisierungen verfügbar sind.

Überprüfen Sie bitte regelmäßig, ob es Aktualisierungen der *pfSense* gibt und installieren Sie diese gegebenenfalls.

Öffnen Sie für das Update der Firewall die Startseite über ein Browserfenster. Sie erreichen die Seite über die URL https://firewall.paedml-linux.lokal.

Melden Sie sich als Benutzer Administrator mit dem zugehörigen Kennwort an.

Auf der Startseite wird angezeigt, wenn Aktualisierungen verfügbar sind („Update available“). Unter „Click Here to view update.“ versteckt sich der Link, der angeklickt werden muss, um das Update anzustoßen.

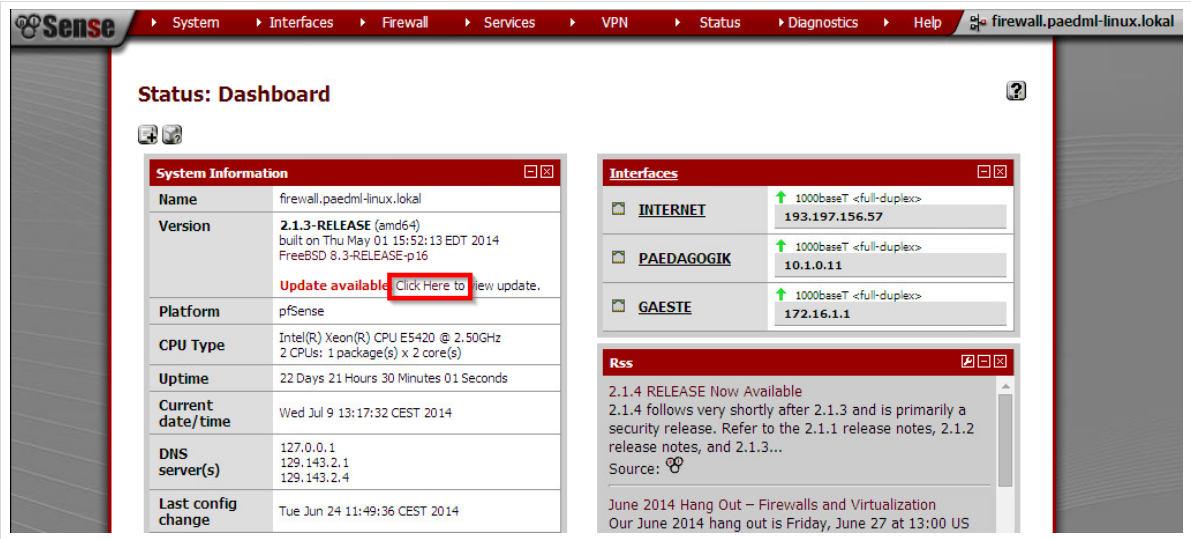


Abb. 152: Aufruf der pfSense-*Startseite mit verfügbarem Update*

Auf den nächsten Seite werden Informationen zu dem verfügbaren Update angezeigt. Über den Knopf „*Invoke Auto Upgrade*“ können sie di Systemaktualisierung starten.

Wenn die Checkbox „*Perform full backup prior to upgrade*“ aktiviert wurde, wird vor dem Upgrade eine Sicherung der Konfiguration angelegt.

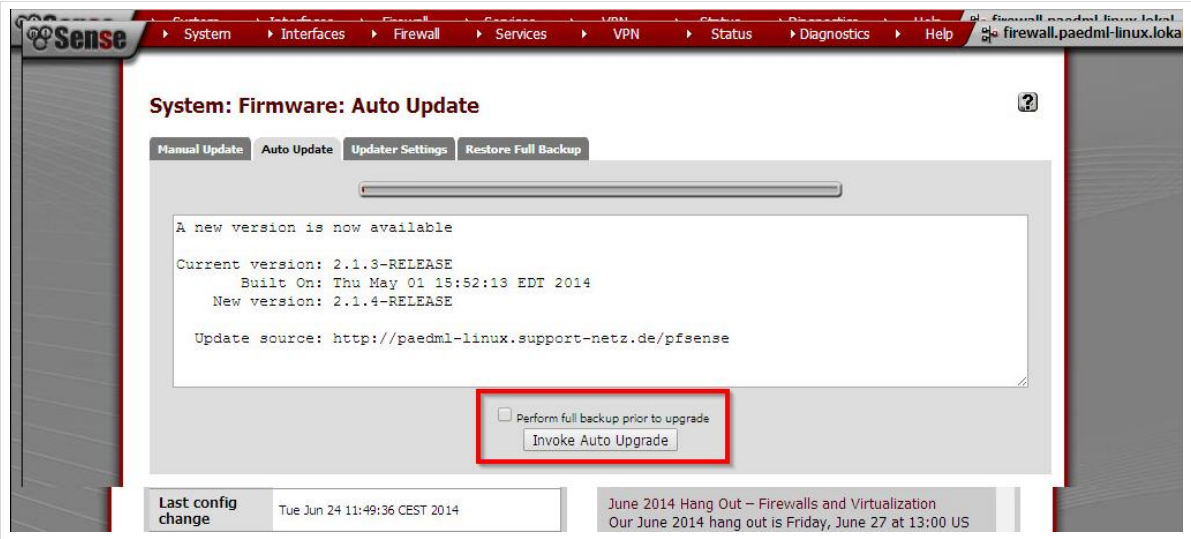


Abb. 153: Start des Upgrades über den entsprechenden Schalter

Im Anschluss wird das Update heruntergeladen…

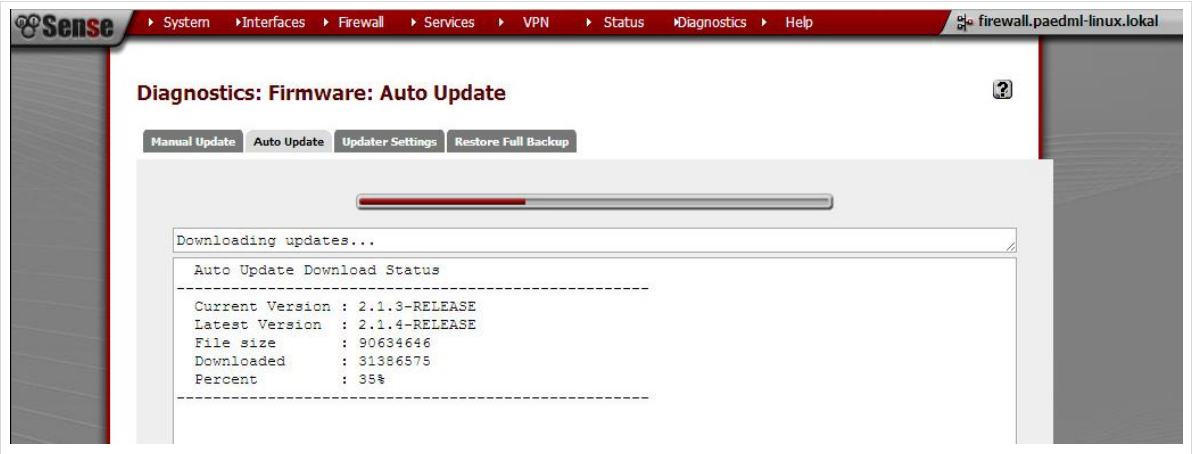


Abb. 154: Die Aktualisierungen werden heruntergeladen

… und installiert. Nach der Installation wird die Firewall neu gestartet.

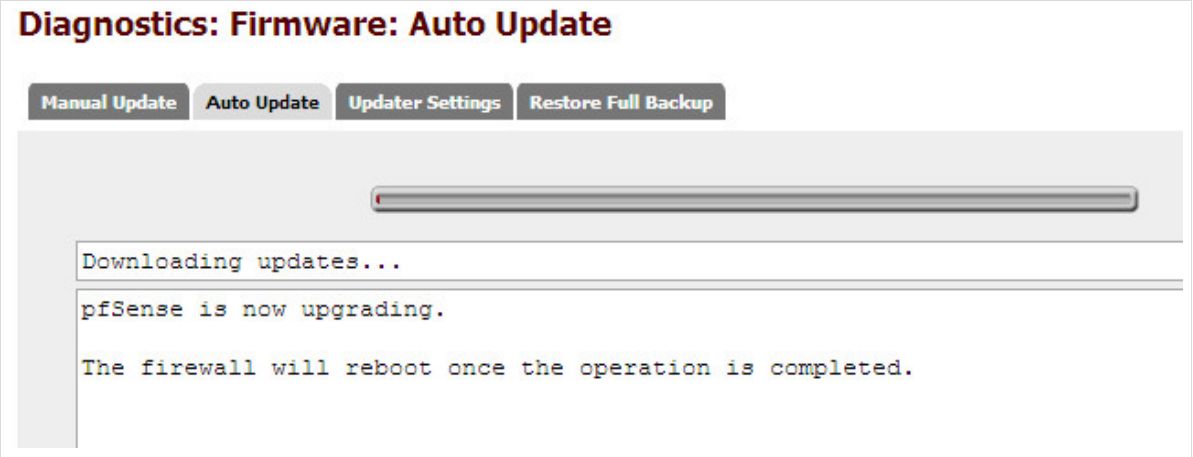


Abb. 155: Anzeige eines Neustarts der pfSense

Schalten Sie die Firewall während des Updatevorgangs auf keinen Fall aus!

5.5 OpenVM-Tools aktualisieren

Nach jedem Update der Firewall müssen Sie die open-vm-tools (die Open Source Variante der vmware-Tools) auf der Firewall auffrischen.

Dies geschieht über das Firewall-Menü „*System* | *Packages*“. Im Reiter „*Installed Packages*“ finden Sie das Paket „*open-vm-tools*“. Rechts der Tabelle befinden sich drei Symbole. Mit dem mittleren „*pkg*“-Symbol können Sie das Paket neu installieren. Beim Mouseover springt ein Hilfedialog auf „*Reinstall Open-VM-Tools package*“, der anzeigt, dass der richtige Knopf gewählt wurde.

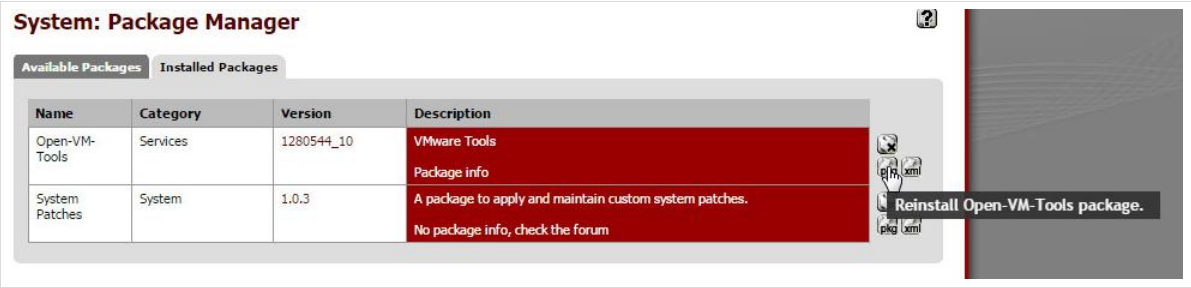


Abb. 156: Neuinstallation von open-vm-tools

Im nächsten Dialog muss die Installation nochmals mittels „*Confirm*“ bestätigt werden.

Abb. 157: Bestätigung der Neuinstallation

6. Ausrollen der VM „AdminVM“

Rolle und Funktion der VM „AdminVM“
Es gibt einige Services für den Betrieb der *paedML Linux* (z.B. die *Windows*-Aktivierung, Gruppenrichtlinien), die auf einem *Windows*-Rechner laufen müssen. Dafür ist die virtuelle Maschine „*AdminVM*“ vorgesehen. Da aus lizenzrechtlichen Gründen kein vorinstalliertes *Windows*-System als OVF-Vorlage ausgeliefert werden darf, enthält die OVF-Vorlage „*AdminVM*“ zwar die Grundkonfiguration der virtuellen Maschine, jedoch noch kein Betriebssystem.

Das Betriebssystem und die benötigte Software kann jedoch in einem automatisierten Prozess installiert werden. Dies wird im Folgenden beschrieben.

6.1 Import der VM aus OVF-Vorlage

Der Import der OVF-Vorlage sollte bereits erfolgt sein, damit steht auf dem Virtualisierungs-Host schon eine virtuelle Maschine (allerdings ohne Betriebssystem) bereit.

Falls der Import der OVF-Vorlage noch nicht erfolgt ist, führen Sie die Kapitel 4.5 (Seite 75) beschriebenen Schritte aus.

6.2 Bereitstellen des Windows-Installationsmediums unter opsi

Bei *opsi* handelt es sich um ein komplexes Produkt zur Softwareverteilung. Im folgenden Kapitel werden nur die notwendigsten Schritte beschrieben, um eine lauffähige *AdminVM* zu erhalten.

Der folgende Abschnitt ist lediglich ein gekürzter Auszug aus dem Administrationshandbuch, umfassendere Informationen zu *opsi* und zur Client-Aufnahme finden sich dort.

Es wird empfohlen für die *AdminVM Windows 7* (64bit) zu verwenden – auch wenn Sie an den anderen Clients im Schul-Netz *Windows 8* oder höher einsetzen. Sie benötigen einen deutschen *Windows 7-Datenträger (64bit)* mit integriertem *Service Pack 1.*

1. Loggen Sie sich auf dem Management-PC per *vSphere-Client* auf dem Virtualisierungs-Host ein.
2. Legen Sie die *Windows*-Installations-DVD in das Laufwerk des Management-PCs ein.
3. Öffnen Sie im *vSphere-Client* die Konsole der virtuellen Maschine „*opsi-Server*“ (bzw. „*backup*“).
4. Verbinden Sie das virtuelle CD-Laufwerk der VM „*opsi-Server*“ mit der im Management-PC eingelegten CD/DVD.

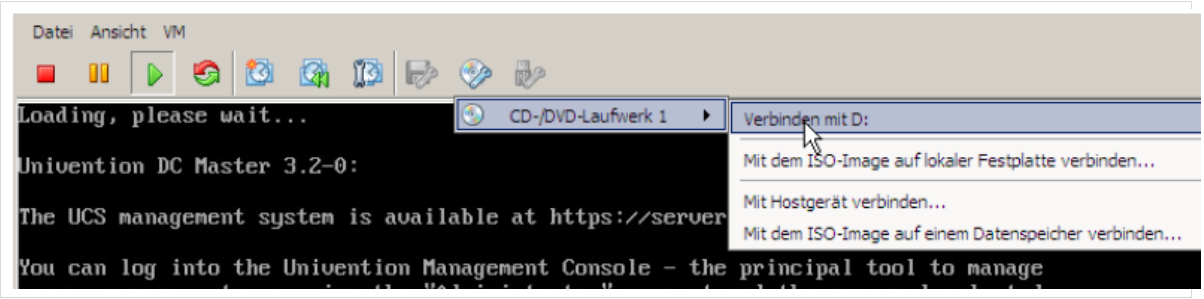

Datei Ansicht VM
Loading, please wait...
Univention DC Master 3.2-0:
The UCS management system is available at https://server
You can log into the Univention Management Console - the principal tool to manage
CD-/DVD-Laufwerk 1
Verbinden mit D:
Mit dem ISO-Image auf lokaler Festplatte verbinden...
Mit Hostgerät verbinden...
Mit dem ISO-Image auf einem Datenspeicher verbinden...

*Abb. 158: Die DVD des Management-PCs wird virtuell in das Laufwerk der VM „*opsi-*Server“ eingelegt*

5. Melden Sie sich als Benutzer „*root*“ auf der VM „*opsi-Server*“ an.
6. Binden Sie die CD in das Dateisystem ein („mounten“):

```
# mount /cdrom
```

7. Kopieren Sie die Dateien des Installationsmediums in das angegebene Verzeichnis.

```
#cp -r /cdrom/* /var/lib/opsi/depot/opsi-local-image-win7-x64/installfiles
```

8. Hängen Sie die CD wieder aus:

```
#umount /cdrom
```

9. Setzen Sie die erforderlichen Rechte im *opsi*-Dateisystem:

```
#opsi-set-rights /var/lib/opsi/depot/opsi-local-image-win7-x64/installfiles
```

10. Danach kann die „virtuelle CD“ wieder von der VM „*opsi-Server*“ getrennt werden, indem Sie im *vSphere-Client* auf das CD-Icon klicken und das Laufwerk trennen.
11. Nun kann das Installationsmedium aus dem Laufwerk des Management-PCs entnommen werden.

6.3 Aufnahme der AdminVM über die Schulkonsole

Starten Sie die virtuelle Maschine „*AdminVM*“ über den *vSphere-Client*:

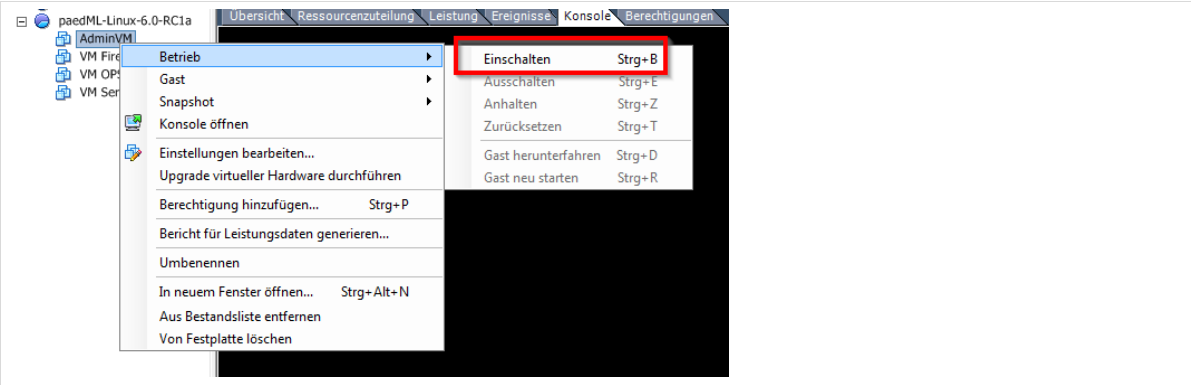


Abb. 159: Start der VM „AdminVM“

Öffnen Sie die Konsole der virtuellen Maschine durch Rechtsklick auf „*AdminVM*“:

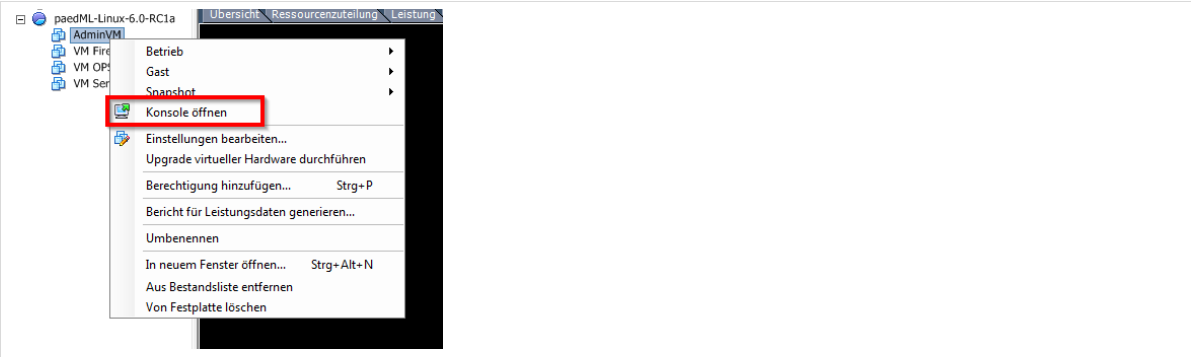


Abb. 160: Öffnen der Konsole.

Die virtuelle Maschine sollte nun über das Netzwerk booten. Gegebenenfalls muss zuvor die Bootreihenfolge der virtuellen Maschine in deren BIOS geändert werden. Um in das BIOS von virtuellen Maschinen zu gelangen, drücken Sie gleich nach dem Einschalten der virtuellen Maschine auf die F2-Taste.

Network boot from Intel E1000
Copyright (C) 2003-2008 VMware, Inc.
Copyright (C) 1997-2000 Intel Corporation
CLIENT MAC ADDR: 00 50 56 CA FE 08 GUID: 564D3204-82CA-C91C-7920-5F70AF488B92
CLIENT IP: 10.1.0.238 MASK: 255.255.255.0 DHCP IP: 10.1.0.1
GATEWAY IP: 10.1.0.11
PXELINUX 4.02 debian-20110423 Copyright (C) 1994-2010 H. Peter Anvin et al
!PXE entry point found (we hope) at 9E95:0106 via plan A
UNDI code segment at 9E95 len 0BDE
UNDI data segment at 98FF len 5960
Getting cached packet 01 02 03
My IP address seems to be 0A00100EE 10.1.0.238
ip=10.1.0.238:10.1.0.1:10.1.0.11:255.255.255.0
BOOTIF=01-00-50-56-ca-fe-08
SYSUUID=564d3204-82ca-c91c-7920-5f70af488b92
TFTP prefix:
Trying to load: pxelinux.cfg/default ok
Loading ucc-1.0-lmz-desktop-image.img.kernel.....
Loading ucc-1.0-lmz-desktop-image.img.initrd.....

Abb. 161: Die virtuelle Maschine „AdminVM“ bootet per PXE

Die virtuelle Maschine bootet nun in ein UCC[3] Live-System:

[3] *Univention Corporate Client*

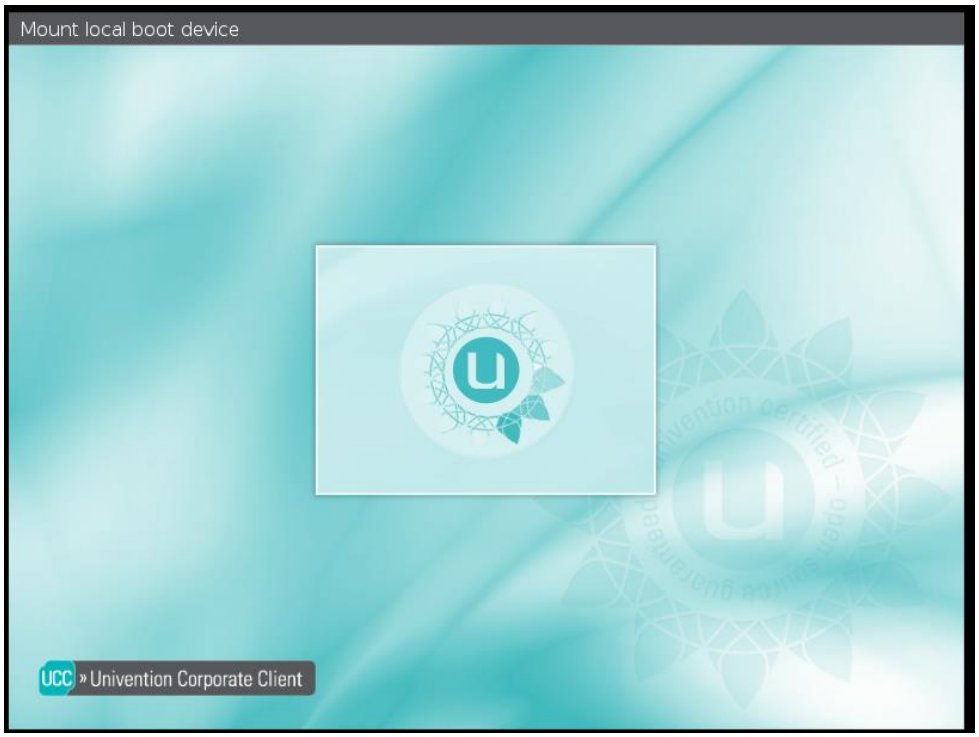


Abb. 162: Laden des UCC-Live-Systems

Wenn das Live-System gebootet ist, öffnet sich automatisch ein Browser und Sie werden mit der Schulkonsole verbunden. Melden Sie sich als Benutzer „*domadmin*“ mit dessen Passwort an.

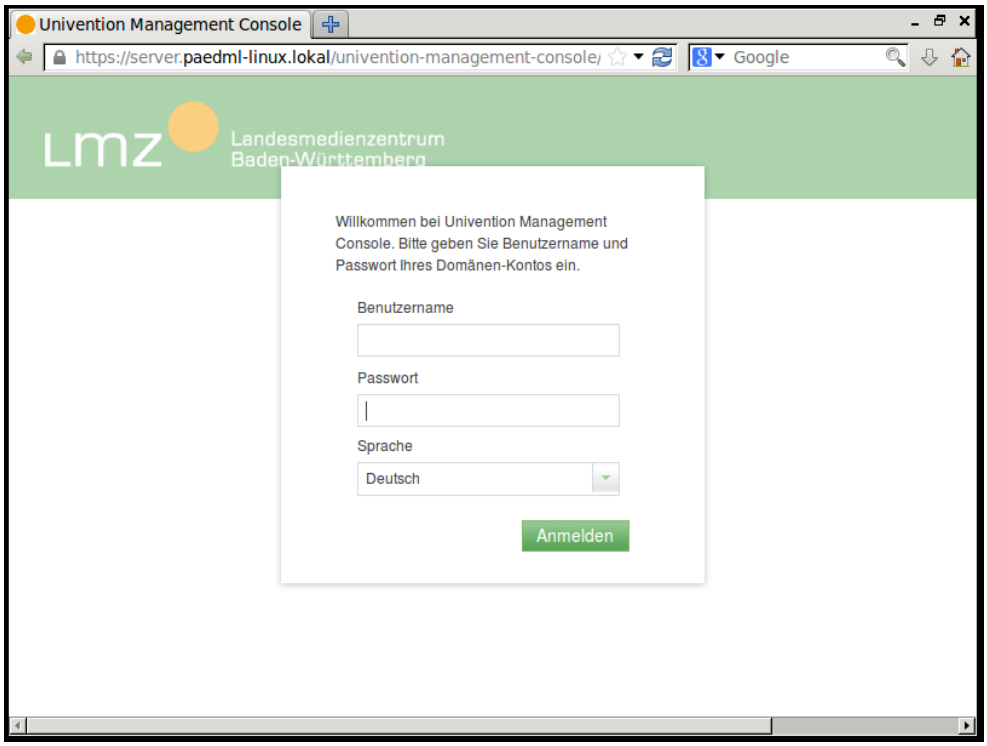


Abb. 163: Anmelden an der Schulkonsole als Benutzer „domadmin“

Im ersten Schritt müssen Sie auswählen, welcher *System-Typ* dem aufzunehmenden Gerät zugewiesen werden soll. Bei der *AdminVM* handelt es sich um ein Gerät des Typs „*Windows-System*“. Wenn Sie die die Auswahl getroffen haben, drücken Sie auf „*Weiter*“, um zur nächsten Maske zu gelangen.

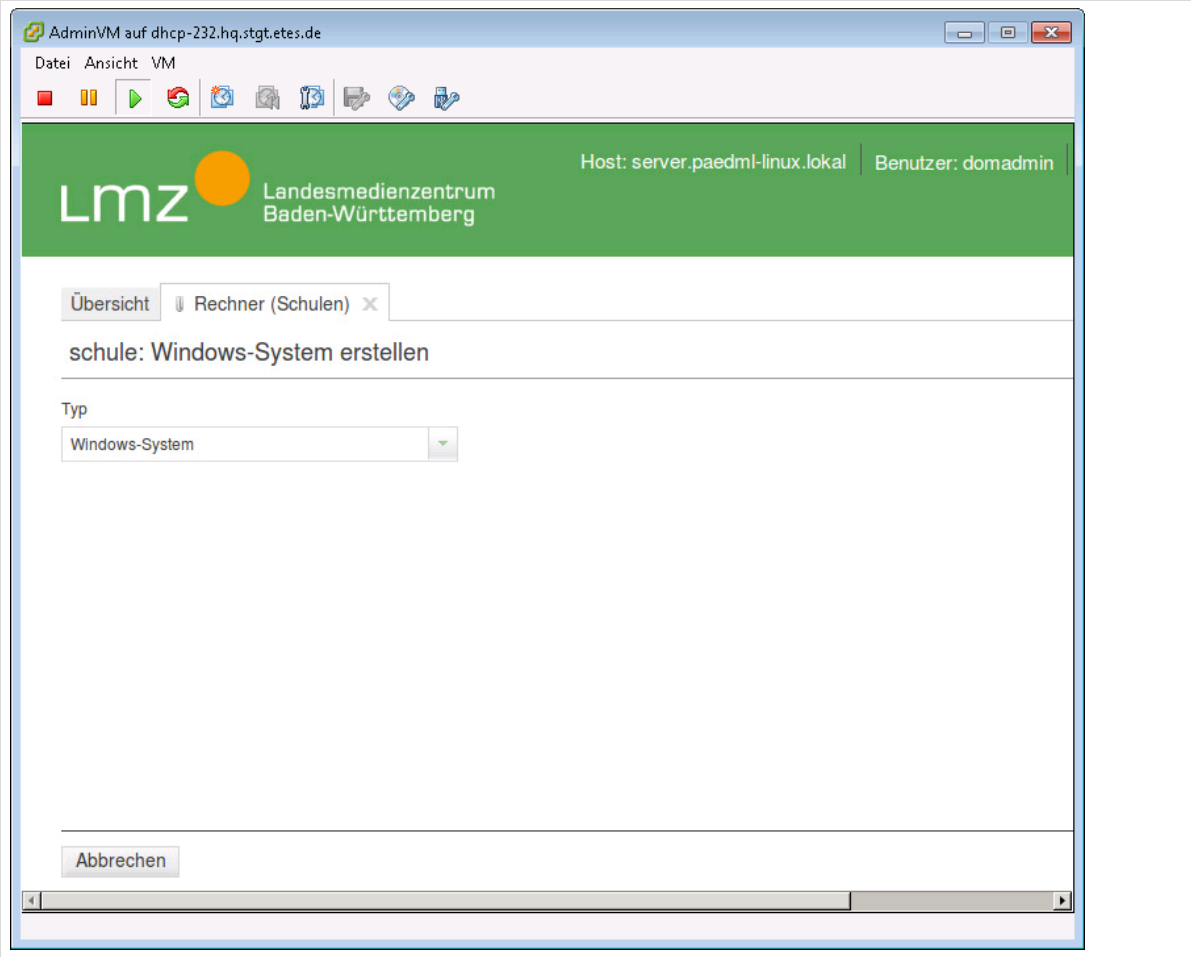


Abb. 164: Auswahl des System-Typs

Tragen Sie in der Maske „*Erstellen eines neuen Computers*“ die folgenden Einstellungen ein:

- Rechnername: `adminvm`
- IP-Adresse: `10.1.0.13`
- Subnetzmaske: `255.255.255.0`

Klicken Sie auf „*Weiter*“.

Weichen Sie keinesfalls von diesen Vorgaben ab, da die virtuelle Maschine *adminvm* sonst nicht sauber in das System integriert wird.

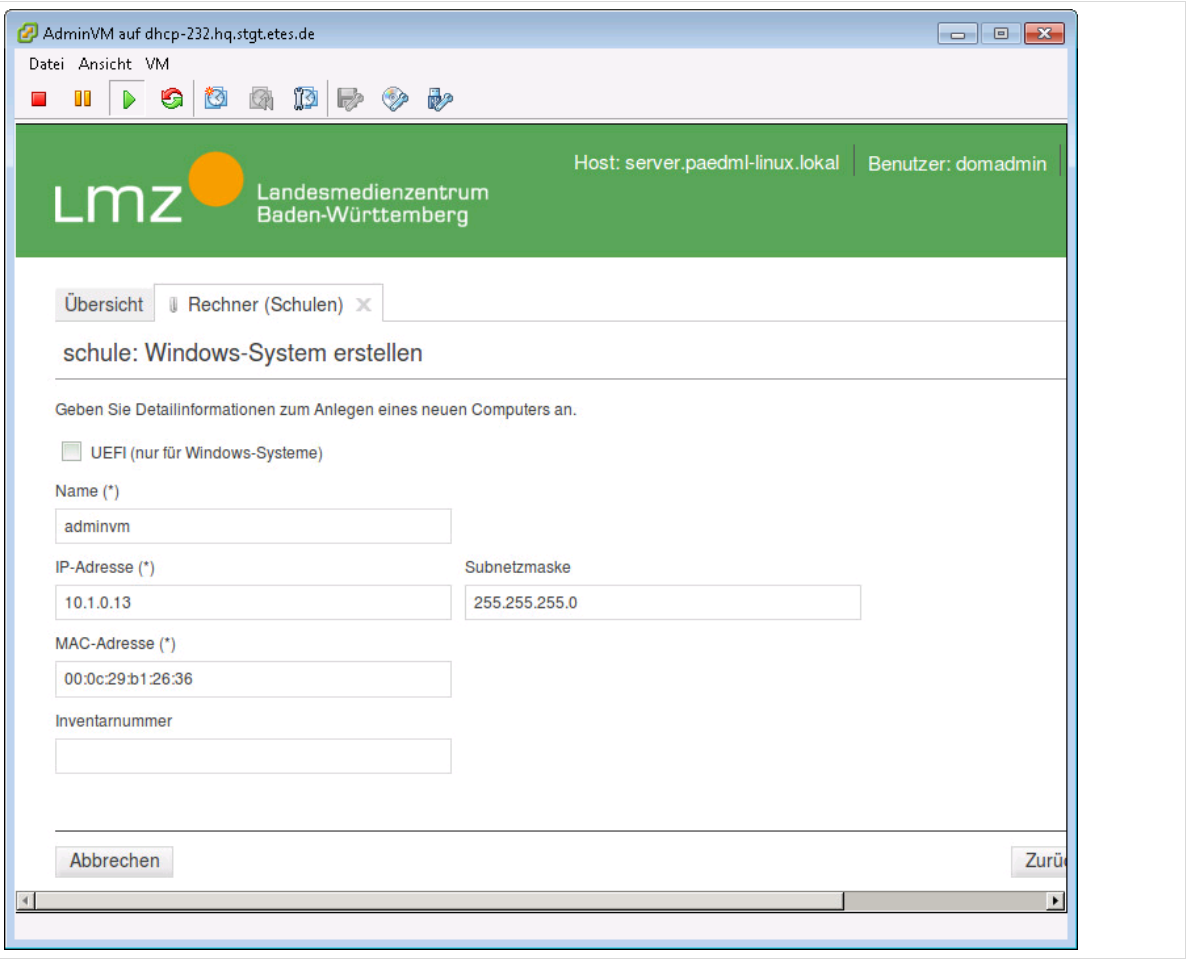


Abb. 165: Aufnahme der VM „AdminVM“ über die Schulkonsole

Wenn der Computer erfolgreich aufgenommen wurde, wird dies wie folgt angezeigt:

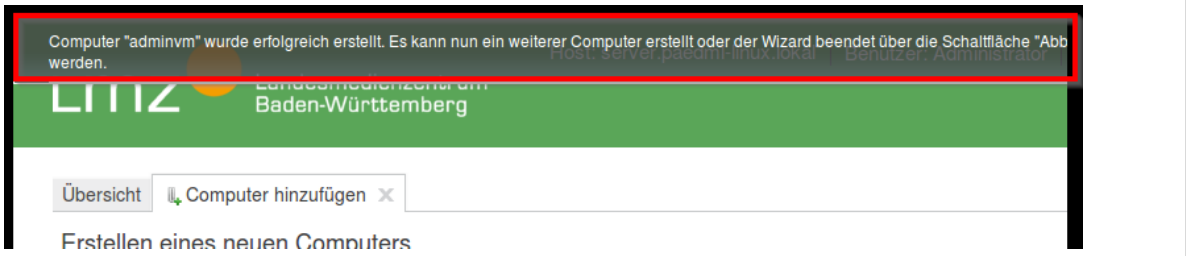

Computer "adminvm" wurde erfolgreich erstellt. Es kann nun ein weiterer Computer erstellt oder der Wizard beendet über die Schaltfläche "Abb
werden.
Baden-Württemberg
Übersicht
Computer hinzufügen
Erstellen eines neuen Computers

Abb. 166: Erfolgreiche Aufnahme der „AdminVM“

Sie können sich anschließend von der Schulkonsole abmelden, lassen Sie den Browser jedoch für die nächsten Schritte geöffnet.

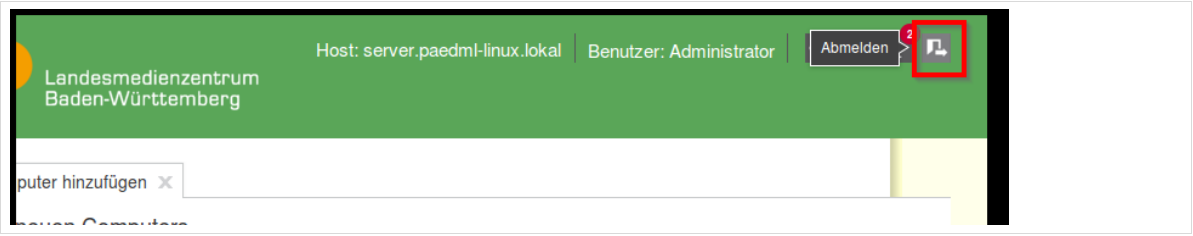


Abb. 167: Abmelden von der Schulkonsole

6.4 Einstellungen in opsi

Der *opsi* -Server muss so konfiguriert werden, dass nach dem Ausrollen des Betriebssystems die notwendige Software auf der *AdminVM* installiert wird.

6.4.1 Anmelden im opsi-configed

Der Browser der *AdminVM* sollte vom letzten Arbeitsschritt noch geöffnet sein.

Wenn Sie vor dem Einrichten der *AdminVM* bereits Rechner in das pädagogische Netz aufgenommen haben, dann können Sie die folgenden Schritte auch auf einem dieser Rechner ausführen.

Noch bequemer als der Zugriff auf die *opsi*-Oberfläche via Webbrowser ist die Arbeit mit einem lokal installierten *opsi-configed*. Dies wird im Administrator-Handbuch beschrieben.

Öffnen Sie im Browser in einem neuen Tab die Adresse http://backup.paedml-linux.lokal:4447/configed

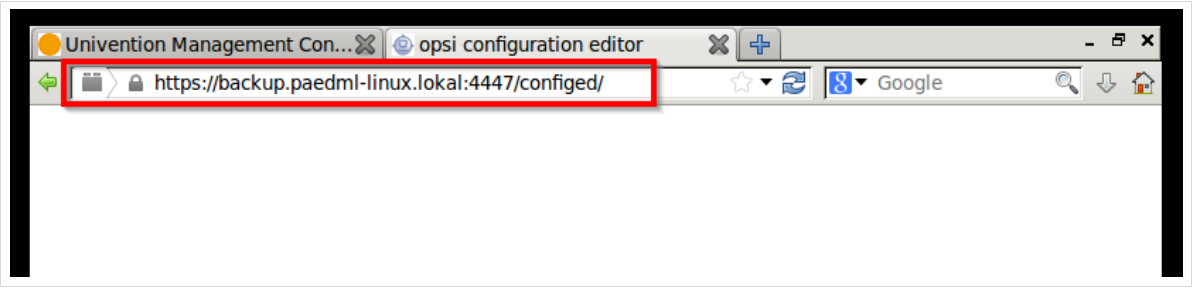


Abb. 168: Öffnen des opsi *configed aus dem Browser der AdminVM*

Klicken Sie auf „*IcedTea-Web aktivieren*“:

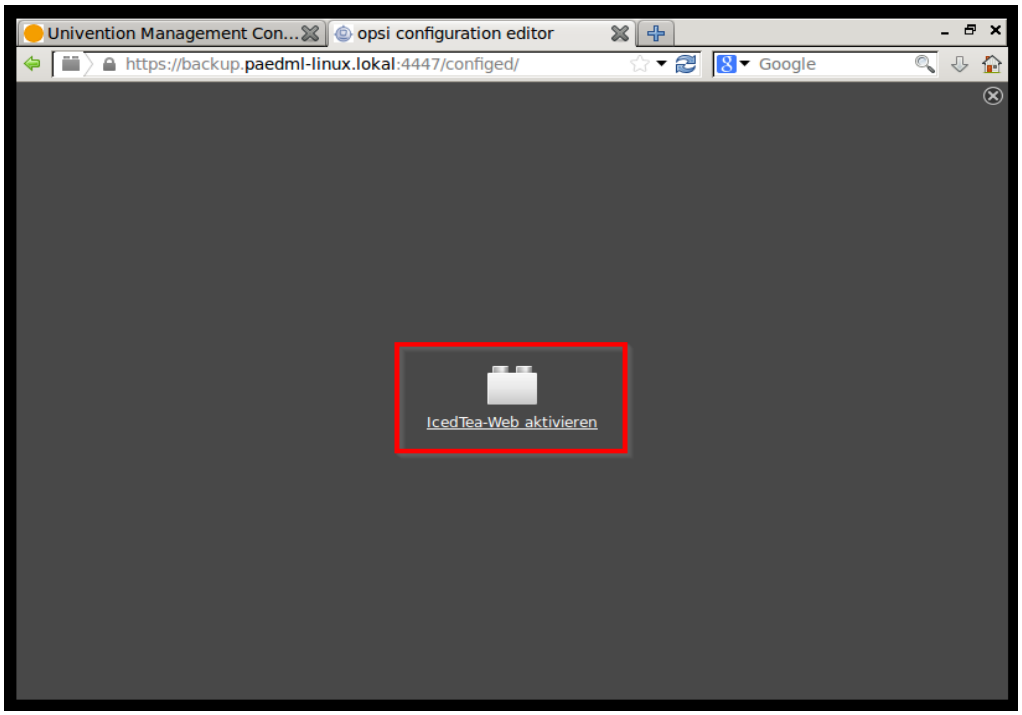


Abb. 169: Aktivieren des Java-Plug-Ins „IcedTea Web“

Bestätigen Sie den folgenden Dialog mit „*Erlauben und Entscheidung merken*“:

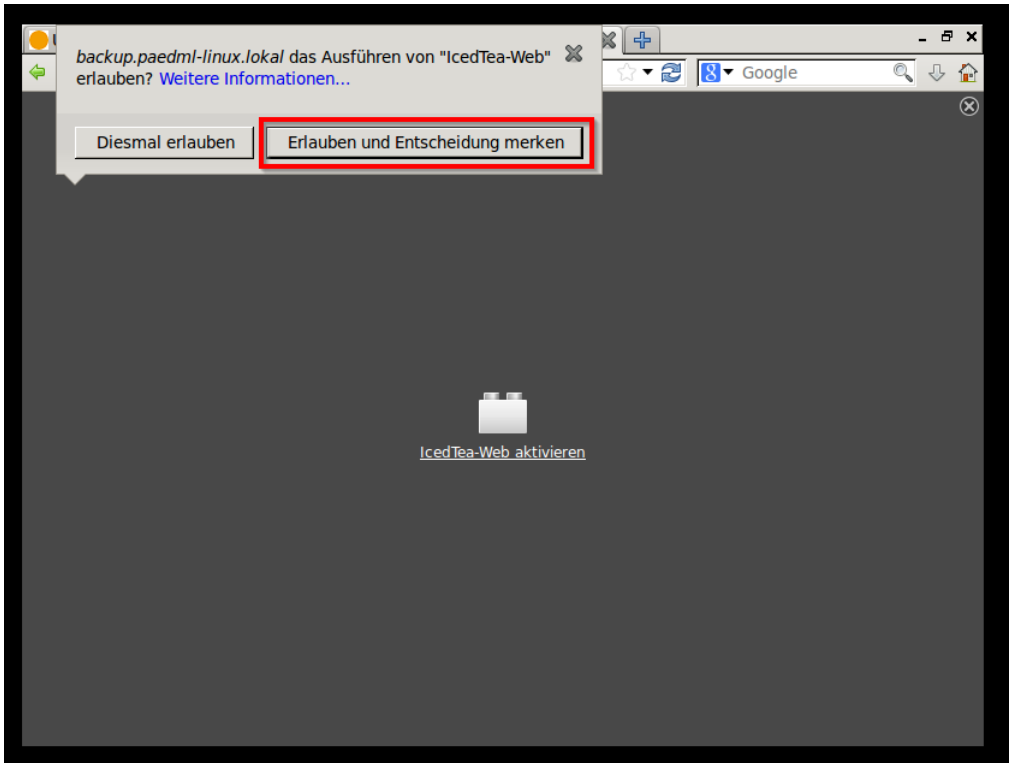


Abb. 170: Java-Plug-In im Browser erlauben

Es erscheinen drei weitere (optisch weitgehend ähnliche) Sicherheitswarnungen, die alle durch Klick auf „*Run*“ bestätigt werden müssen. Außerdem muss die Checkbox vor„*Always trust content from this publisher*“ aktiviert werden:

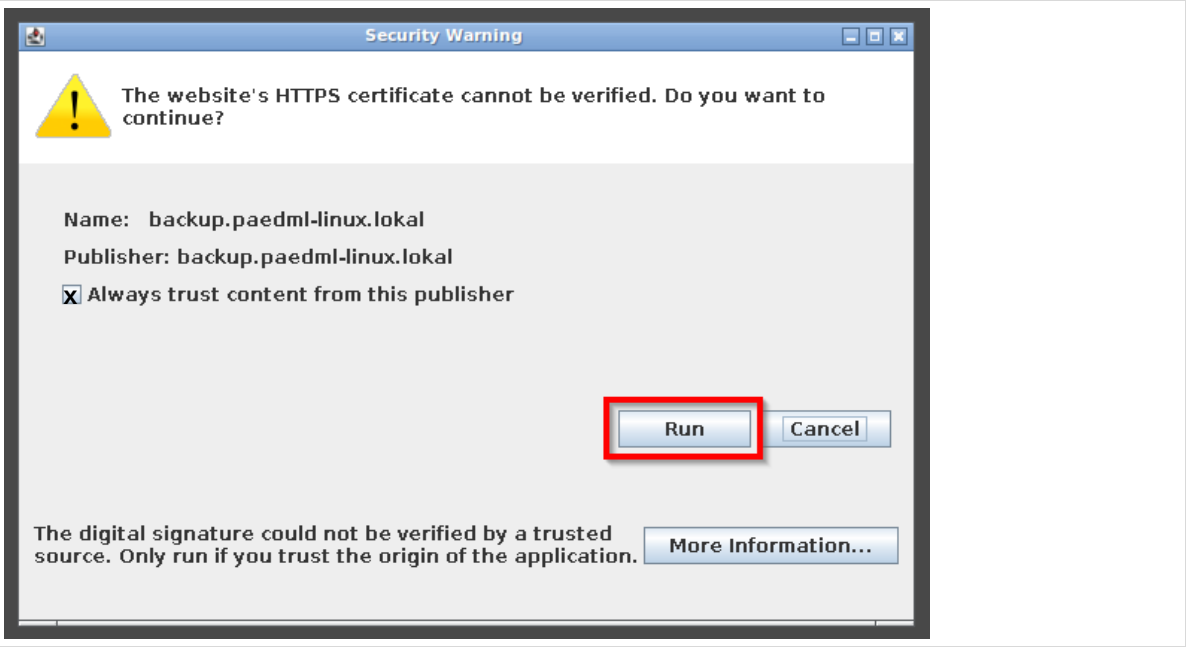

Security Warning
The website's HTTPS certificate cannot be verified. Do you want to continue?
Name: backup.paedml-linux.lokal
Publisher: backup.paedml-linux.lokal
Always trust content from this publisher
Run
Cancel
The digital signature could not be verified by a trusted source. Only run if you trust the origin of the application.
More Information...

Abb. 171: Eine der drei Sicherheitswarnungen.

Gegenüber dem *opsi configed* müssen Sie sich als Benutzer „*Administrator*“ (**Achtung:** großes „A“!) mit ihrem Kennwort authentifizieren:

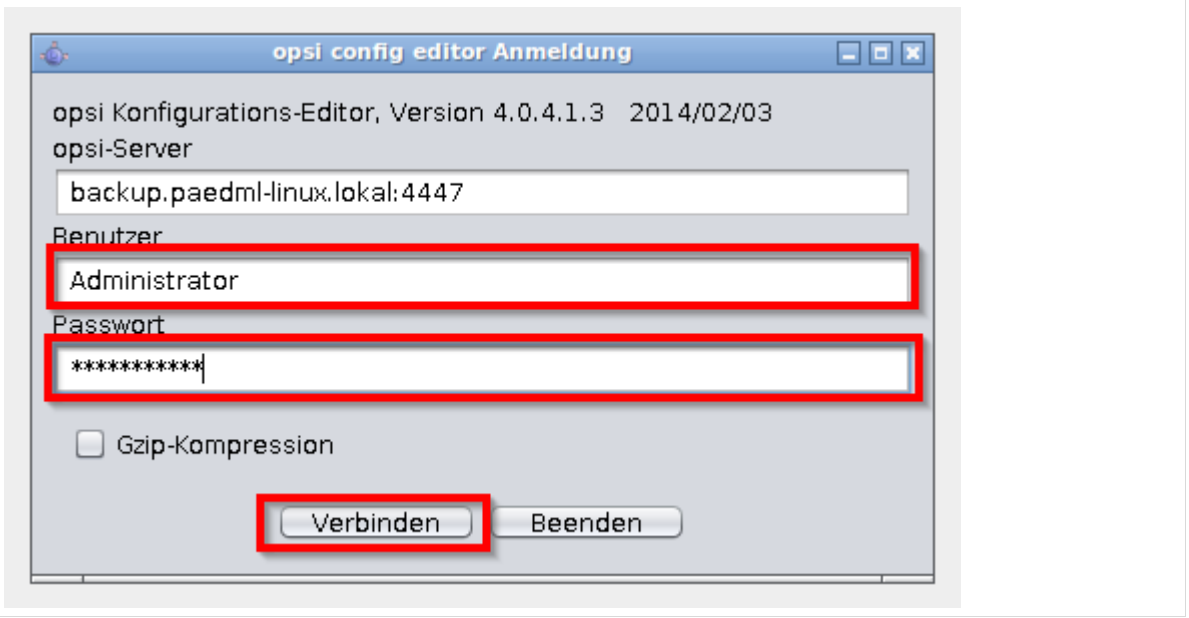


Abb. 172: Authentifizieren am opsi *configed.*

Nach erfolgreicher Anmeldung sehen Sie die Oberfläche des *opsi configed*.

6.4.2 Konfiguration der AdminVM

Markieren Sie im Reiter „*Clients*“ die Maschine „*adminvm.paedml-linux.lokal*“

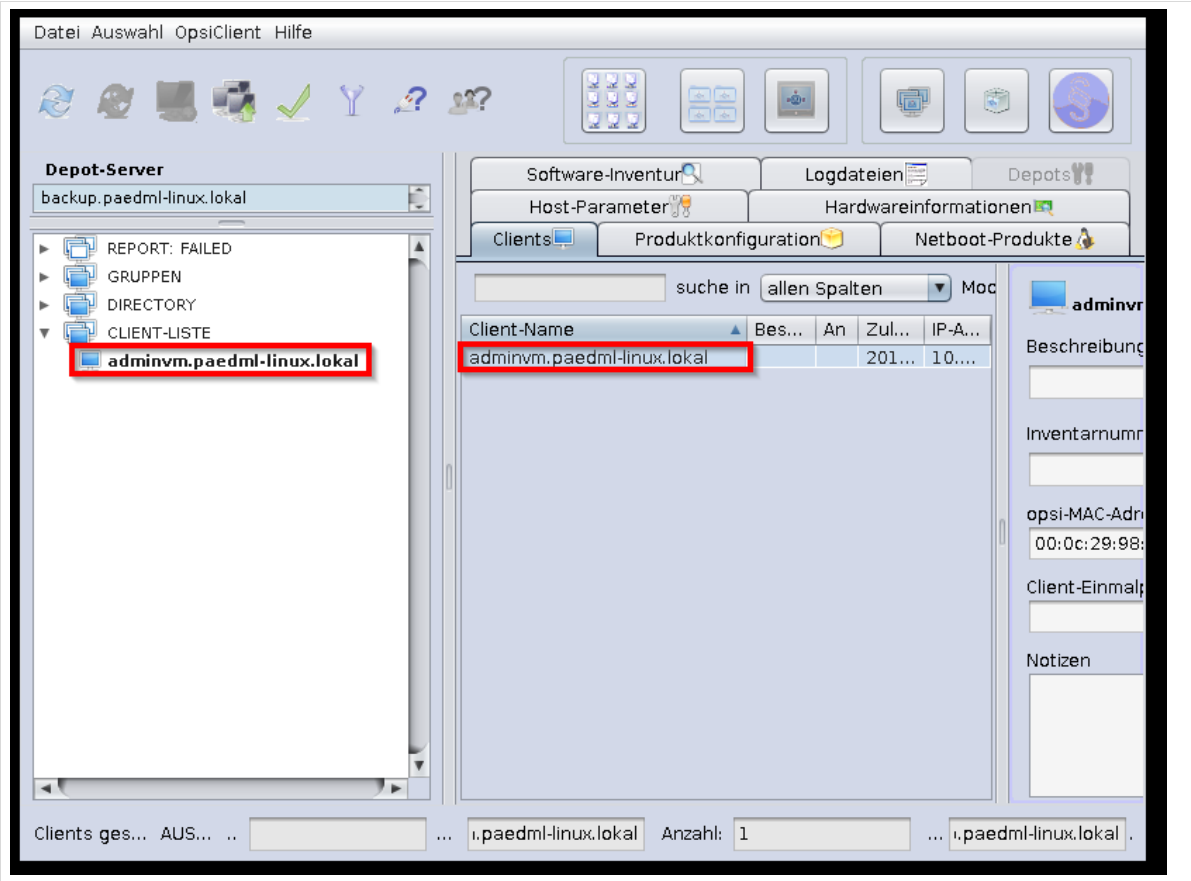


Abb. 173: Auswahl der Maschine „adminvm“

Navigieren Sie in den Reiter „*Netboot-Produkte*“ und setzen Sie Den „*Angefordert*“-Status des Produkts „*opsi-local-image-prepare*“ auf „*setup*“.

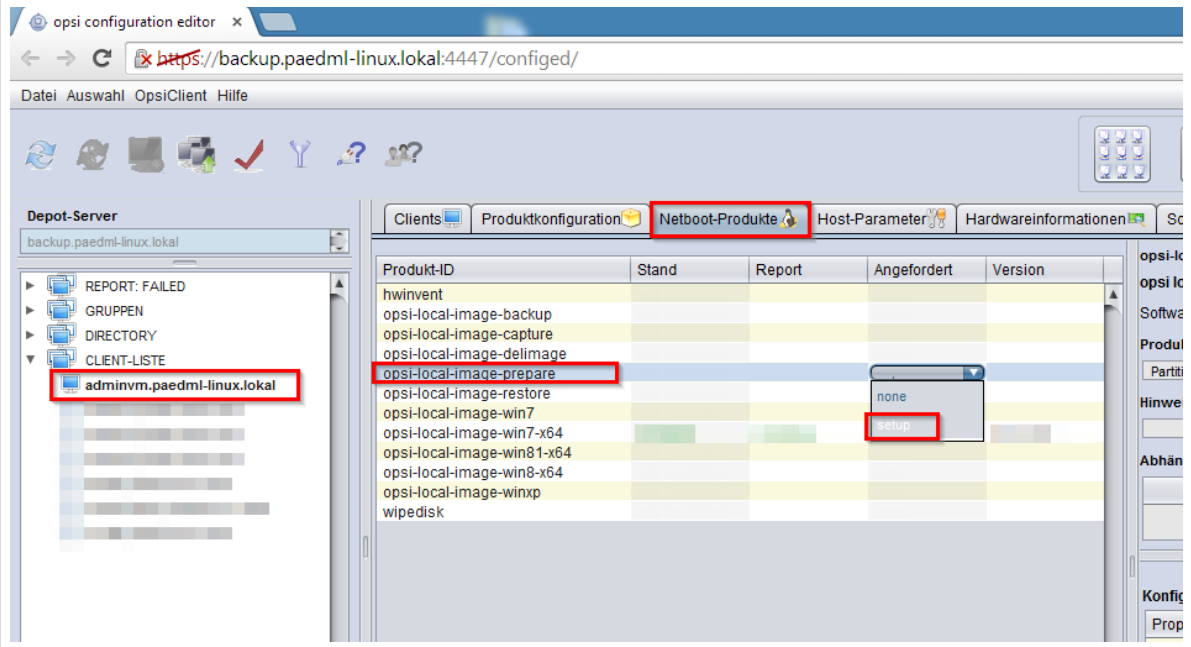


Abb. 174: Anfordern des Setups von opsi-*local-image-prepare*

Kontrollieren Sie rechts unten im Bereich „*Konfiguration für Client*“, ob die Property-Werte wie in der folgenden Abbildung eingestellt sind und ändern Sie diese gegebenenfalls.

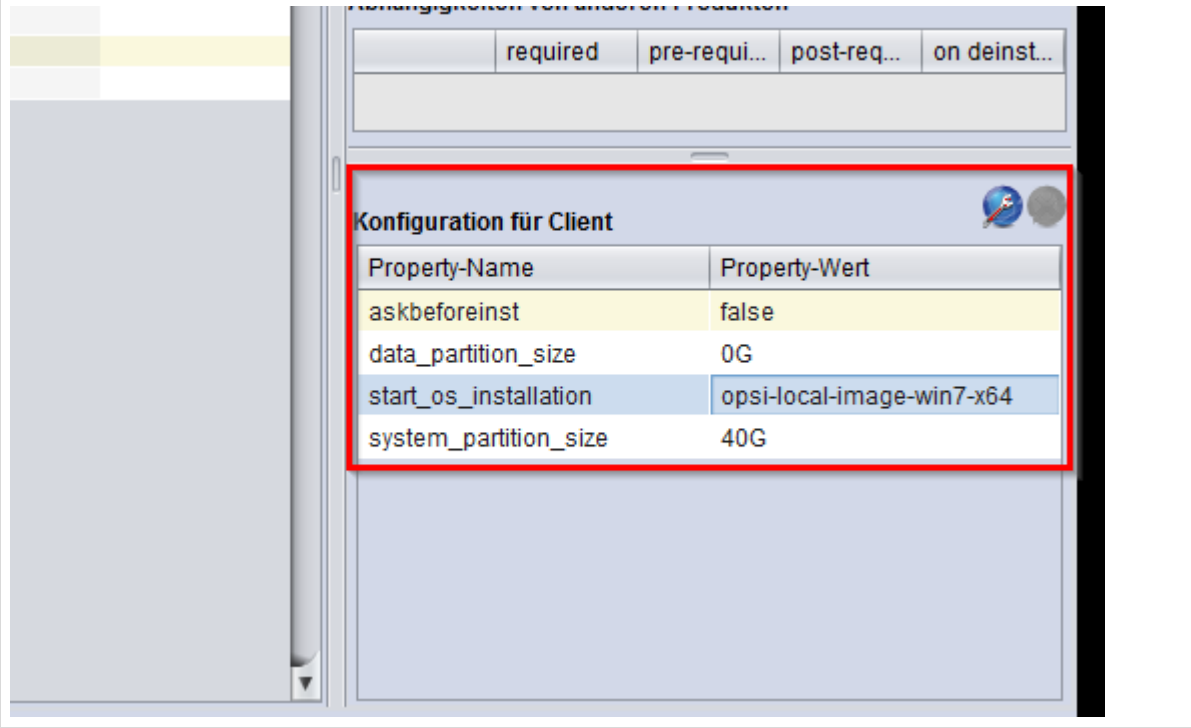


Abb. 175: Kontrolle der Property-Werte für die AdminVM

Navigieren Sie in den Reiter „*Netboot-Produkte*“ und wählen Sie die Zeile „*opsi-local-image-win7-x64*“ aus:

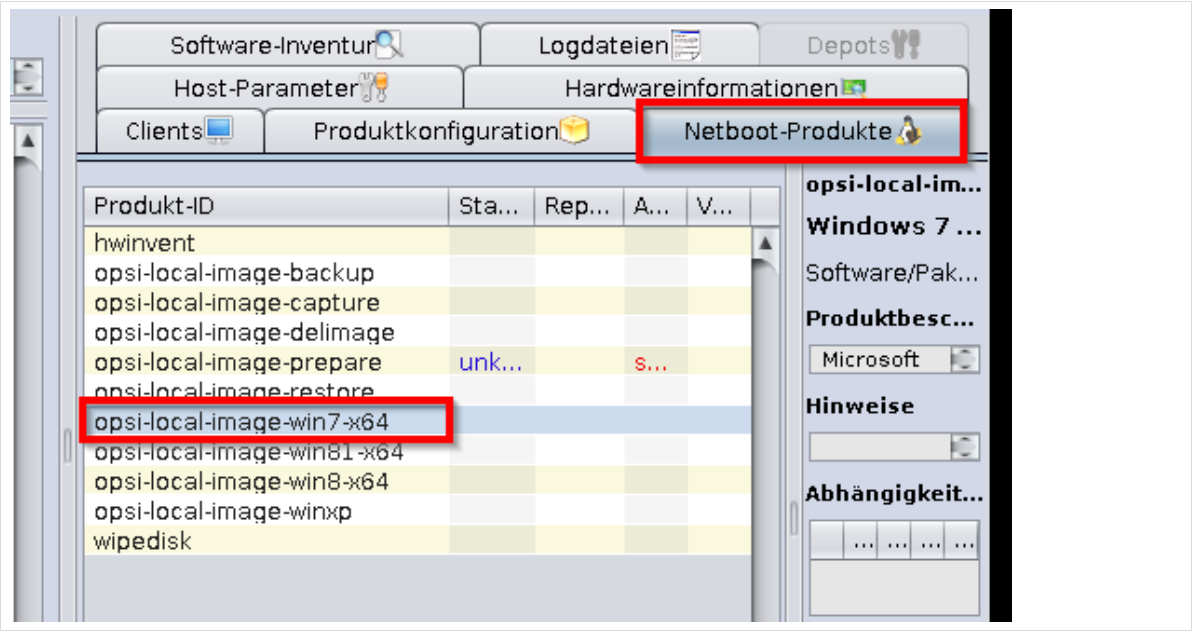


Abb. 176: Auswahl des opsi-*Produkts* „opsi-*local-image-win7-x64*“

Klicken Sie im rechten unteren Bereich („*Konfiguration für Client*“) in die Einstellungen der Zeile „*setup_after_install*“. Dort sollten Sie die Werte „*windomain,clientprodukte*“ vorfinden:

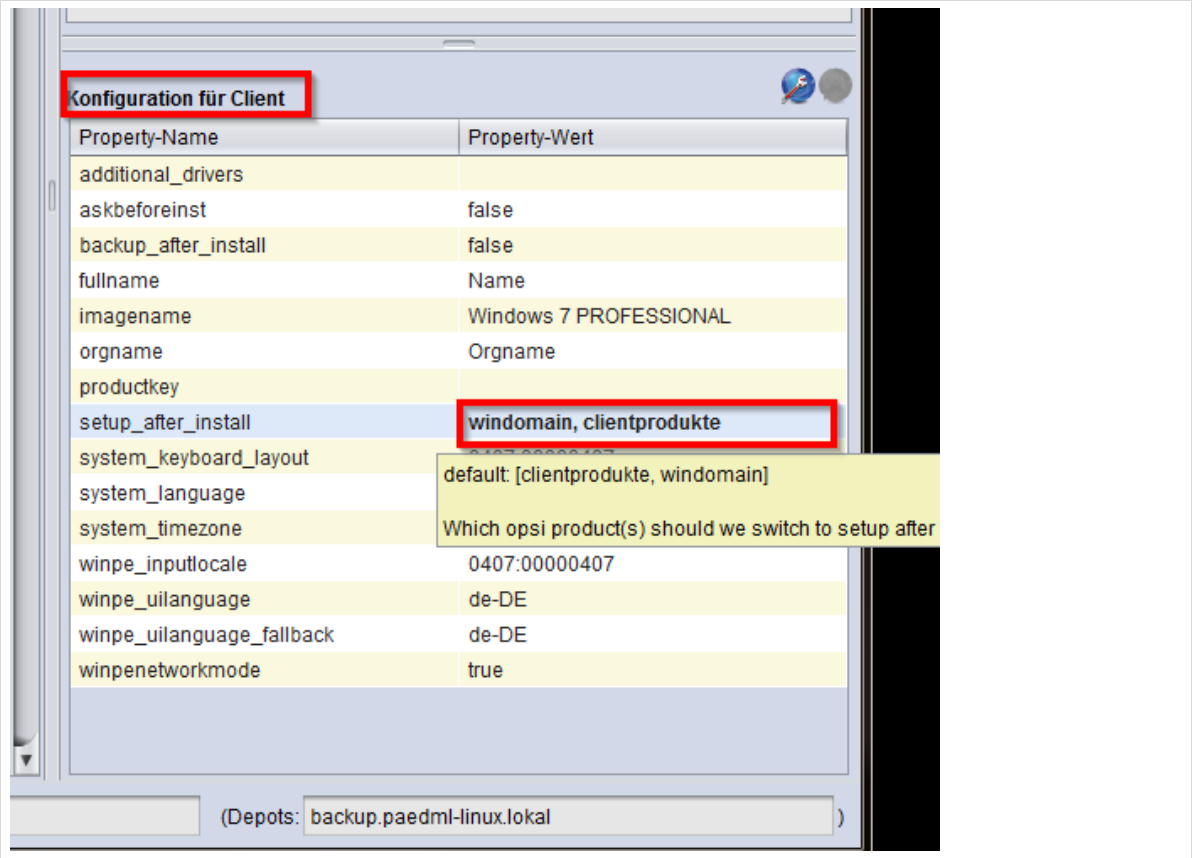


Abb. 177: Verändern des Eintrages unter „setup_after_install“

Tragen Sie im Popup-Fenster in die TextBox den Wert „*adminvm*“ ein, klicken Sie anschließend auf das gelbe Kreuz, um den Wert hinzuzufügen und anschließend auf den Haken:

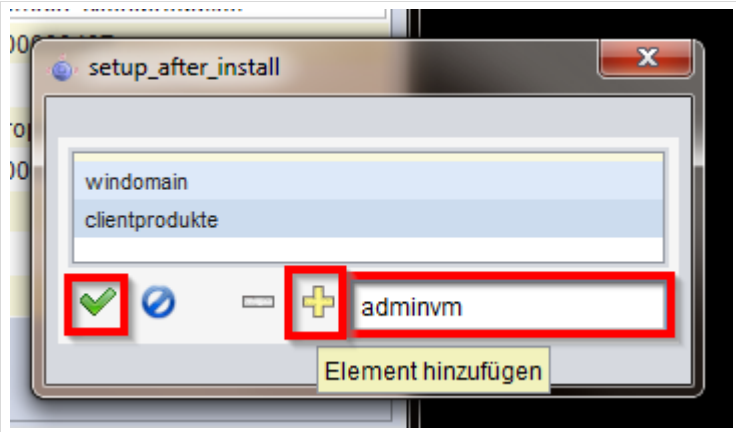


Abb. 178: Hinzufügen des Wertes „adminvm“

Kontrollieren Sie, ob in der Zeile „*setup_after_install*“ nun die drei Werte „*windomain“*, „*clientprodukte*“ und „*adminvm*“ eingetragen sind.

Abb. 179: Die Produkte „windomain“, „clientprodukte“ und „adminvm“ sind zur Installation vorgemerkt.

Zum Abschluss der Konfiguration müssen Sie die eben getätigten Einstellungen durch Klick auf den roten Haken oben links übernehmen:

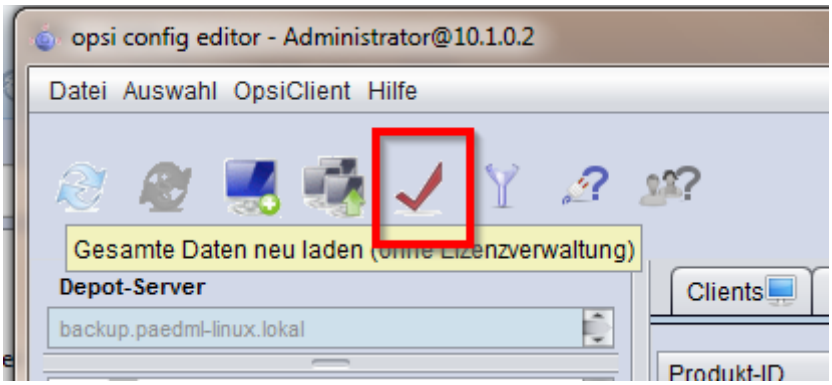


Abb. 180: Übernahme der soeben getätigten Einstellungen.

Nach diesen Änderungen können Sie die VM „*AdminVM*“ ausschalten (z.B. über den vSphere-Client).

6.5 Ausrollen des Betriebssystems

Starten Sie die VM „*AdminVM*“ erneut über den vSphere-Client. Anschließend sollte automatisch das Betriebssystem ausgerollt werden. Nach der Grundinstallation werden automatisch die auf dem *opsi*-Server verfügbaren *Windows*-Updates, sowie einige Softwareprodukte installiert.

Das Ausrollen der AdminVM kann durchaus mehrere Stunden in Anspruch nehmen!

6.6 Installation der VMware-Tools in der AdminVM

Die *VMWare Tools* bieten Vorteile bei der Bedienung virtueller Maschinen (höhere Bildschirmauflösung, bessere Mausunterstützung,…). Außerdem ermöglichen Sie ein geordnetes Herunterfahren virtueller Maschinen, wenn beispielsweise der Hypervisor ausgeschaltet wird.

Aus oben genannten Gründen wird dringend dazu geraten *VMware-Tools* auf allen virtualisierten Geräten zu installieren. Auf den *paedML*-Servern und der Firewall sind die *VMware-Tools* bereits installiert.

Starten Sie die installierte "*AdminVM*" im *vSphere-Client*.

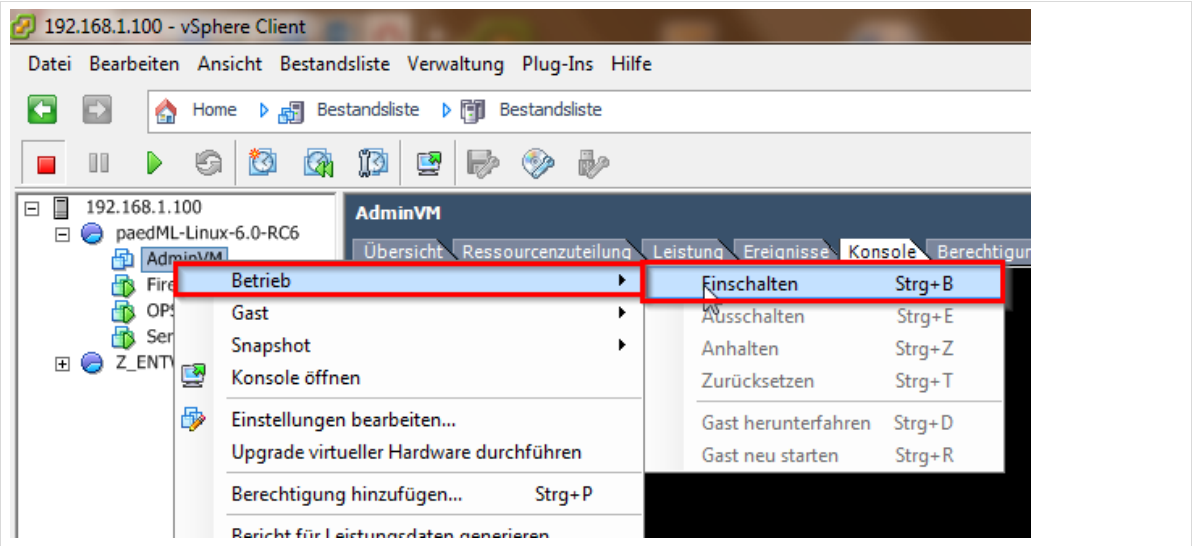


Abb. 181: Starten der VM „AdminVM“

Melden Sie sich als *lokaler Administrator* an (Kennwort: nt123).

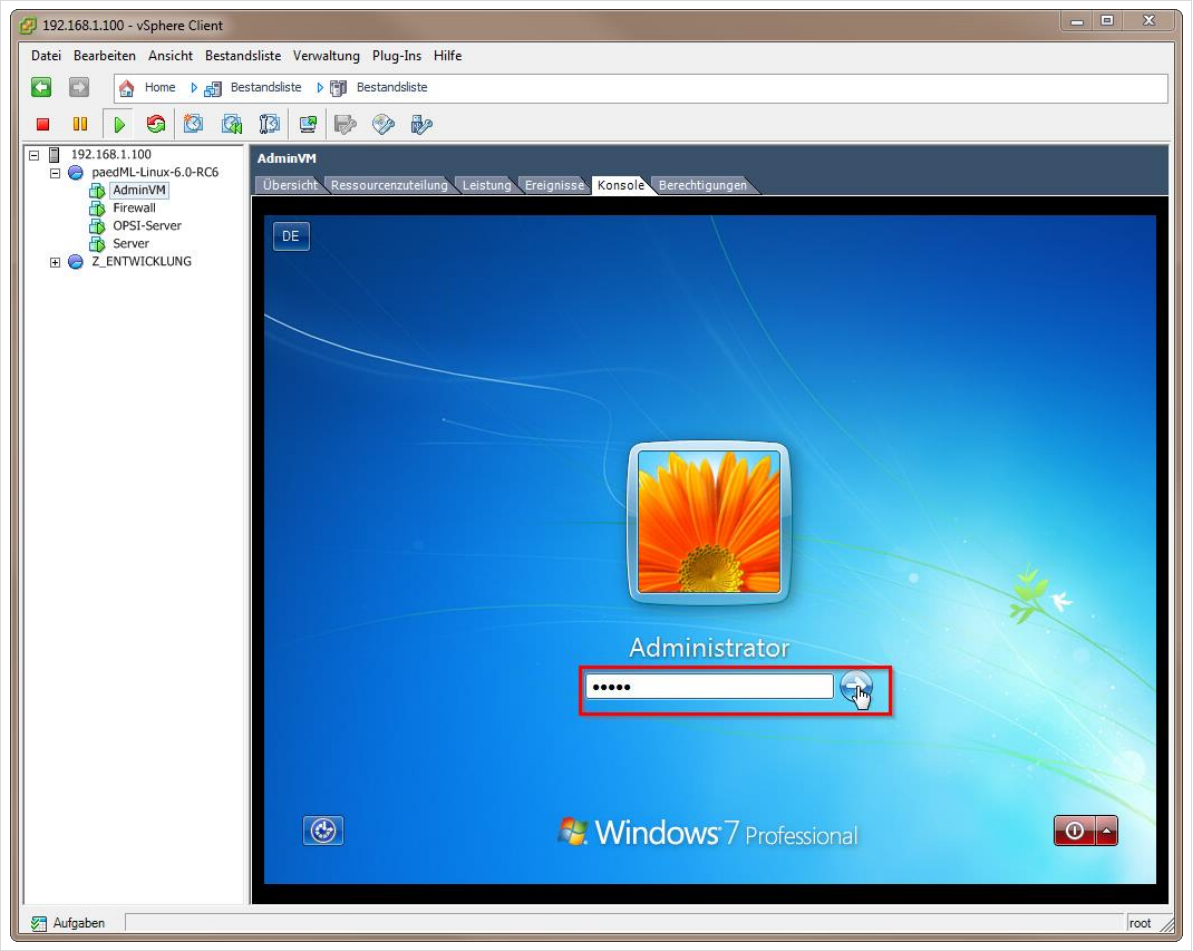


Abb. 182: Anmeldung als lokaler Administrator

Klicken Sie im *vSphere-Client* mit der rechten Maustaste auf die *AdminVM* und Wähleh Sie im Kontextmenü den Punkt "*Gast* | *VMware Tools installieren/aktualisieren*".

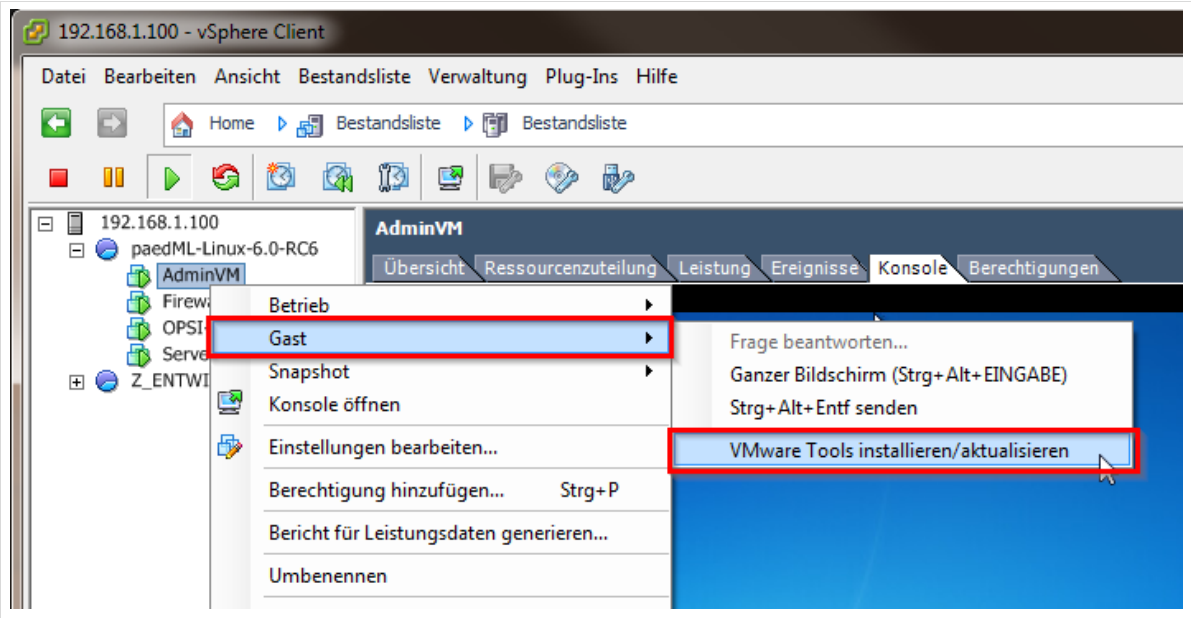


Abb. 183: Auswahl von Installation der VMware Tools

Klicken sie im folgenden Hinweisfenster auf "*OK*".

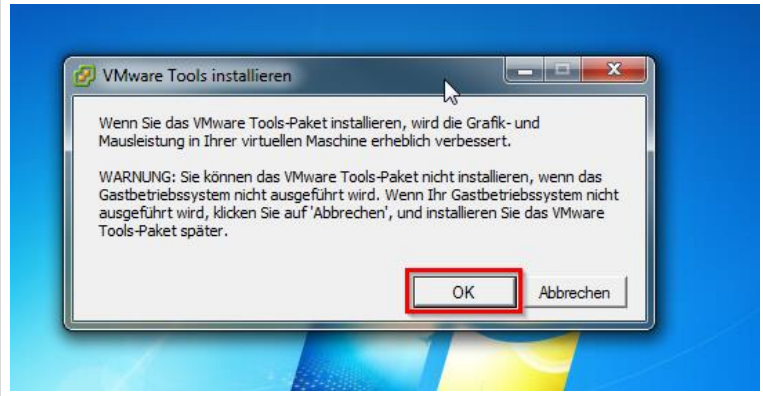

VMware Tools installieren
Wenn Sie das VMware Tools-Paket installieren, wird die Grafik- und Mausleistung in Ihrer virtuellen Maschine erheblich verbessert.
WARNUNG: Sie können das VMware Tools-Paket nicht installieren, wenn das Gastbetriebssystem nicht ausgeführt wird. Wenn Ihr Gastbetriebssystem nicht ausgeführt wird, klicken Sie auf 'Abbrechen', und installieren Sie das VMware Tools-Paket später.
OK
Abbrechen

Abb. 184: Bestätigung der Installation

Daraufhin wird automatisch eine virtuelle DVD mit dem *VMware-Tools*-Installationsprogramm in die *AdminVM* eingelegt und es öffnet sich der dafür typische Windows-Dialog. Wählen Sie die Option "*setup64.exe ausführen*".

Automatische Wiedergabe
DVD-Laufwerk (D:) VMware Tools
Immer für Software und Spiele durchführen:
Programm installieren oder ausführen
setup64.exe ausführen
Veröffentlicht von VMware, Inc.
Ordner öffnen, um Dateien anzuzeigen
mit Windows-Explorer
Weitere Optionen für die automatische Wiedergabe in der Systemsteuerung anzeigen

Abb. 185: Ausführen der Installations-Routine

Damit beginnt der Installationsvorgang der *VMware-Tools.*

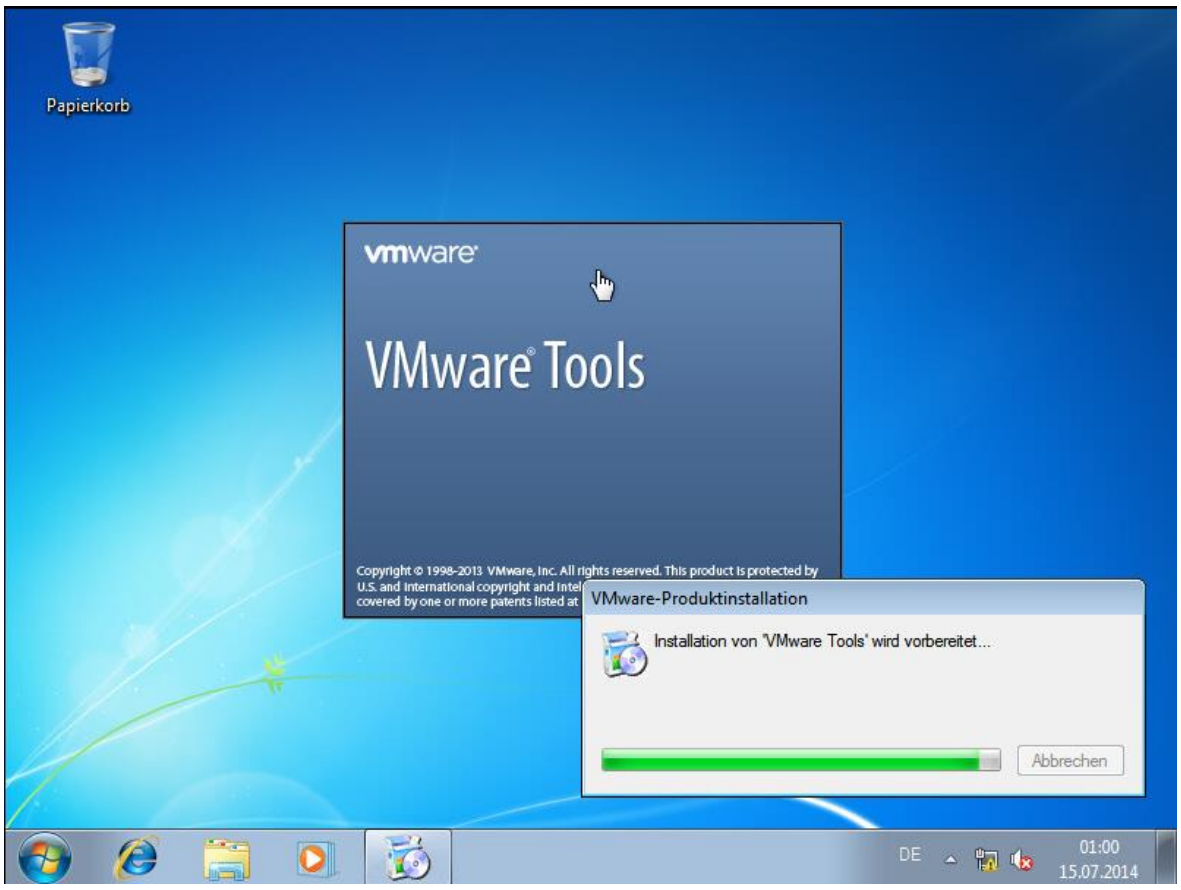


Abb. 186: Die Installation wird gestartet

Klicken Sie im Installations-Assistenzen auf "*Weiter*".

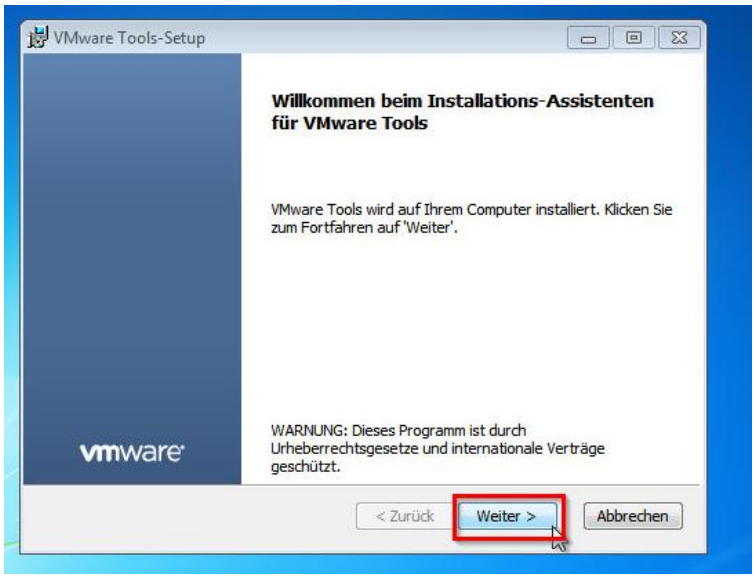

VMware Tools-Setup
Willkommen beim Installations-Assistenten für VMware Tools
VMware Tools wird auf Ihrem Computer installiert. Klicken Sie zum Fortfahren auf 'Weiter'.
WARNUNG: Dieses Programm ist durch Urheberrechtsgesetze und internationale Verträge geschützt.
vmware
< Zurück
Weiter >
Abbrechen

Abb. 187: Installations-Dialog

Übernehmen Sie im nächsten Fenster "*Installationstyp*" die voreingestellte Option "*Standard*" und klicken Sie auf "*Weiter*".

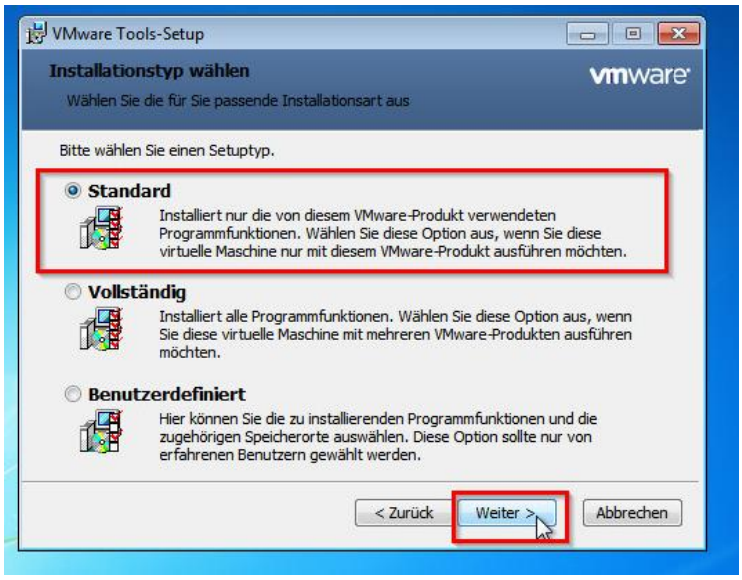

VMware Tools-Setup
Installationstyp wählen
Wählen Sie die für Sie passende Installationsart aus
vmware
Bitte wählen Sie einen Setuptyp.
Standard
Installiert nur die von diesem VMware-Produkt verwendeten Programmfunktionen. Wählen Sie diese Option aus, wenn Sie diese virtuelle Maschine nur mit diesem VMware-Produkt ausführen möchten.
Vollständig
Installiert alle Programmfunktionen. Wählen Sie diese Option aus, wenn Sie diese virtuelle Maschine mit mehreren VMware-Produkten ausführen möchten.
Benutzerdefiniert
Hier können Sie die zu installierenden Programmfunktionen und die zugehörigen Speicherorte auswählen. Diese Option sollte nur von erfahrenen Benutzern gewählt werden.
< Zurück
Weiter >
Abbrechen

Abb. 188: Auswahl der Standard-Installation

Klicken Sie im nächsten Fenster auf "*Installieren*".

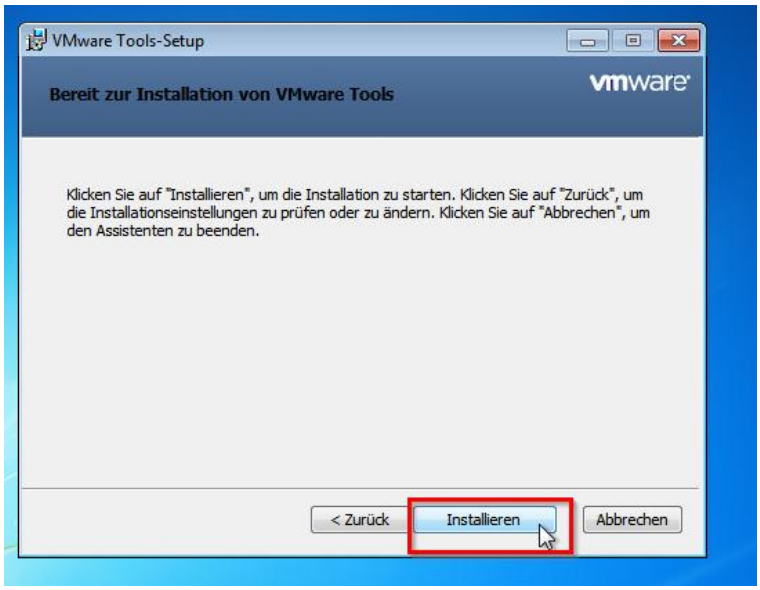

VMware Tools-Setup
Bereit zur Installation von VMware Tools
vmware
Klicken Sie auf "Installieren", um die Installation zu starten. Klicken Sie auf "Zurück", um die Installationseinstellungen zu prüfen oder zu ändern. Klicken Sie auf "Abbrechen", um den Assistenten zu beenden.
< Zurück
Installieren
Abbrechen

Abb. 189: Und noch ein Klick.

Daraufhin beginnt der Installationsvorgang, der einige Minuten in Anspruch nehmen kann.

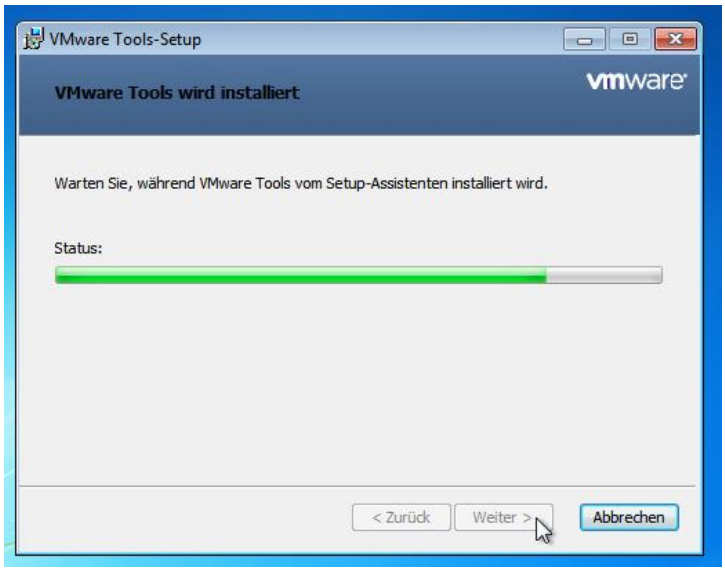


Abb. 190: Die Installation wird ausgeführt.

Der Abschluss der Installation wird durch das folgende Fenster angezeigt, klicken Sie auf "*Fertig stellen*".

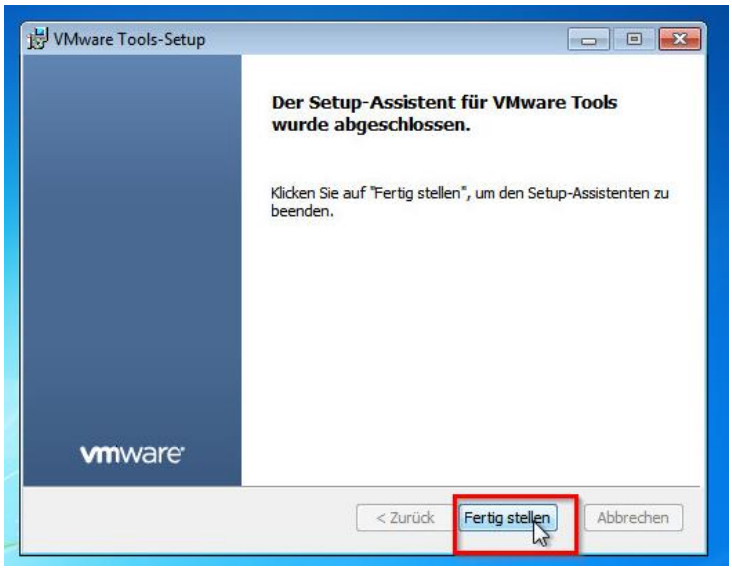


Abb. 191: Fertig stellen der Installation

Sie werden aufgefordert, den Rechner neu zu starten. Klicken Sie auf "*Ja*". Daraufhin wird die *AdminVM* neu gestartet.

Abb. 192: Windows wird gestartet

Wenn die Anmeldemaske wieder erscheint, loggen Sie sich wieder als lokaler Administrator an. Jetzt sind die *VMware-Tools* installiert. Sie erkennen Sie am Icon rechts in der Taskleiste der virtuellen Maschine.

Abb. 193: Anzeige von installierten VMware-Tools

6.7 Ändern der Gruppenzugehörigkeit der AdminVM

Nachdem die VM „*AdminVM*“ in die *paedML* aufgenommen wurde, befindet sie sich unterhalb des LDAP-Containers „*schule*“, in dem sich alle von der *paedML Linux* verwalteten Clients befinden. Diese Clients werden von der *paedML Linux* beispielsweise mit Gruppenrichtlinien versorgt, welche die Rechte auf den Clients einschränken.

Da die AdminVM jedoch fest zum Server-System der *paedML Linux* gehört, muss diese aus dem LDAP-Container „*schule*“ entfernt werden.

Melden Sie sich von einem Browser aus auf der Schulkonsole (https://server.paedml-linux.lokal) als Benutzer „*Administrator*“ mit dem entsprechenden Kennwort an.

Wählen Sie im Menü den Punkt „*Domäne*“ aus und klicken Sie auf „*LDAP-Verzeichnis*“.

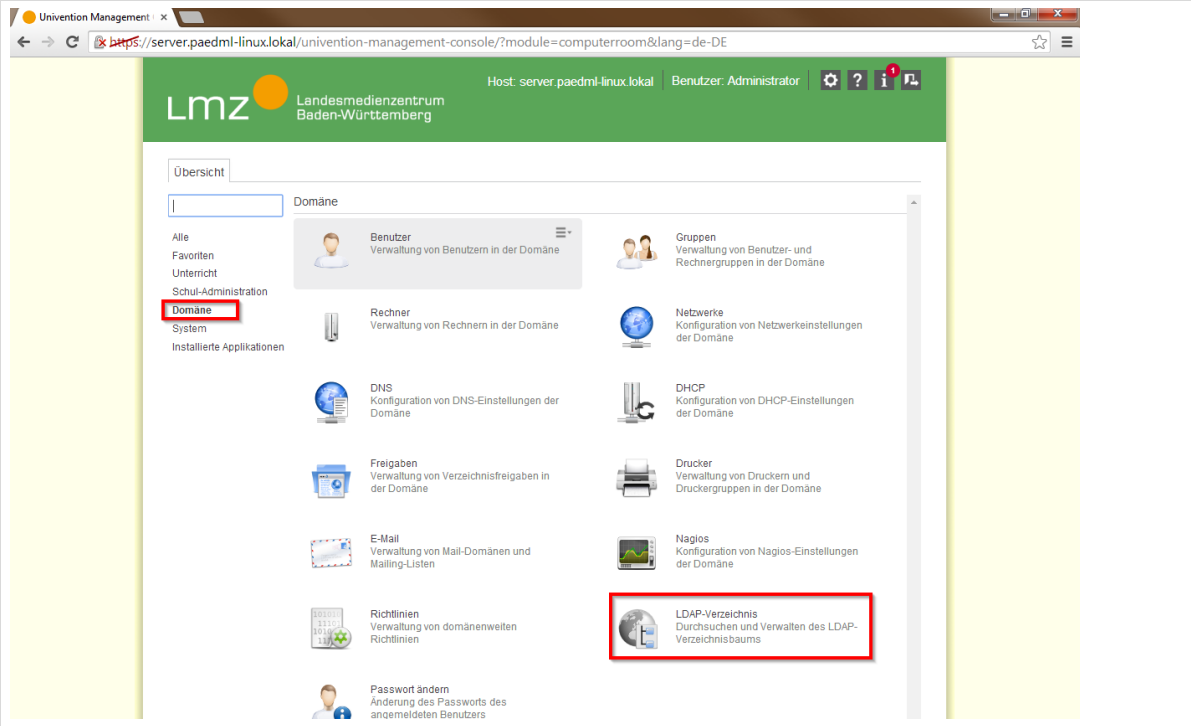


Abb. 194: Verwalten des LDAP-Verzeichnisbaums

Navigieren Sie im LDAP-Verzeichnisbaum zum Ordner „*lokal.paedml-linux/schule/computers*“, markieren Sie das Objekt „*adminvm*“ und klicken Sie auf „*mehr | Verschieben nach…*“:

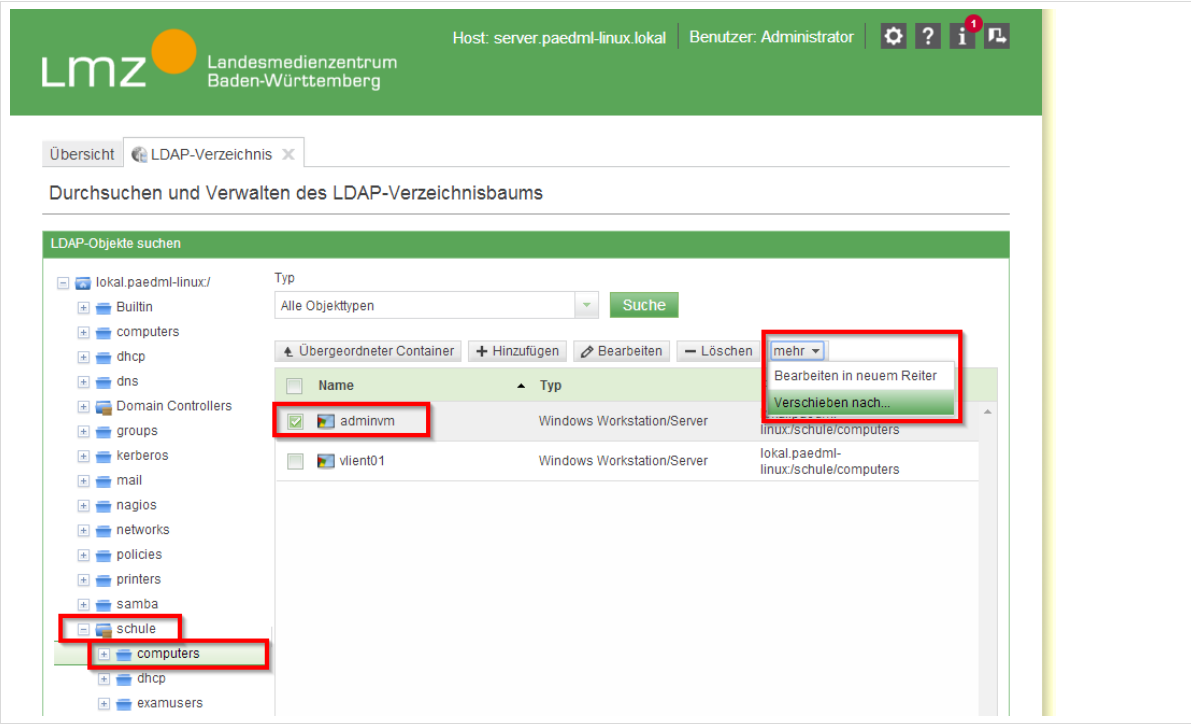


Abb. 195: Verschieben des Objekts „adminvm“ im LDAP-Baum

Wählen Sie im nächsten Fenster den Ordner „*lokal.paedml-linux/computers*“ als Ziel aus und klicken Sie auf „*LDAP-Objekt verschieben*“:

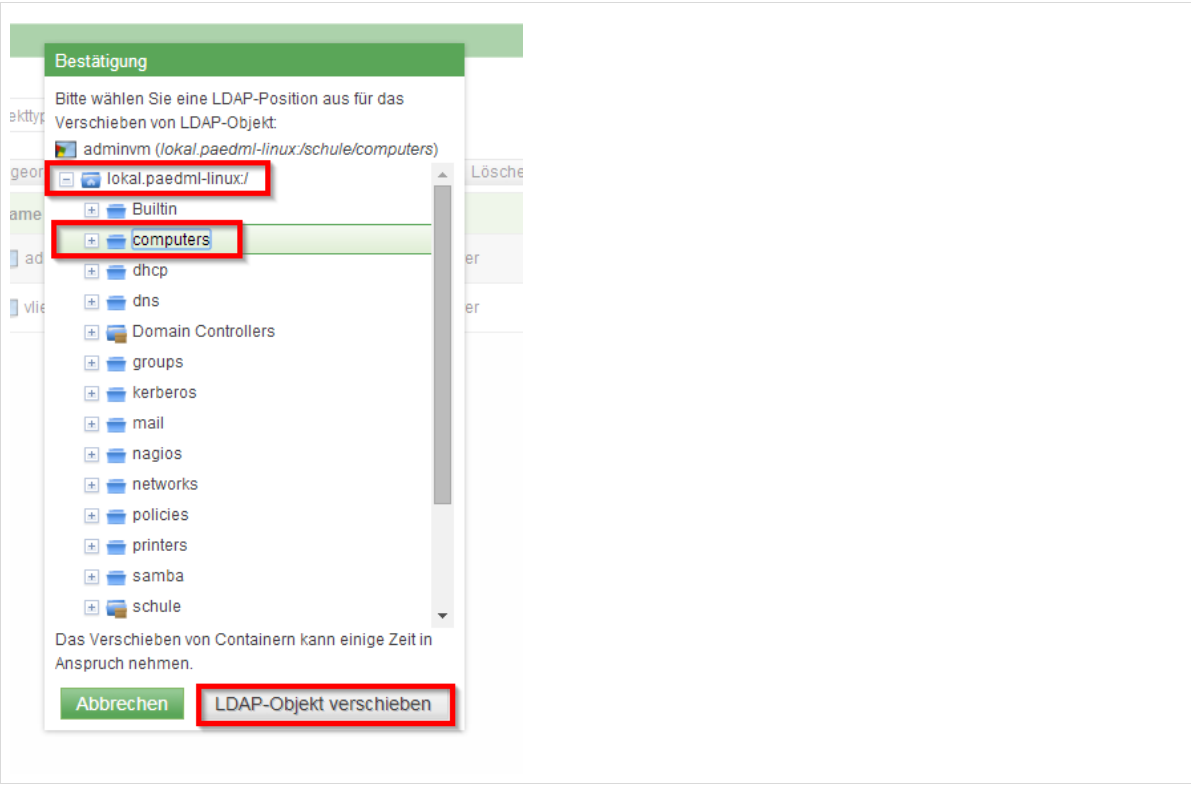


Abb. 196: Auswahl des Ziels im LDAP-Baum

Überprüfen Sie anschließend, ob sich das Objekt „*adminvm*“ wirklich im LDAP-Ordner „*lokal.paedml-linux/computers*“ (**Achtung**: ohne „*schule*“!) befindet.

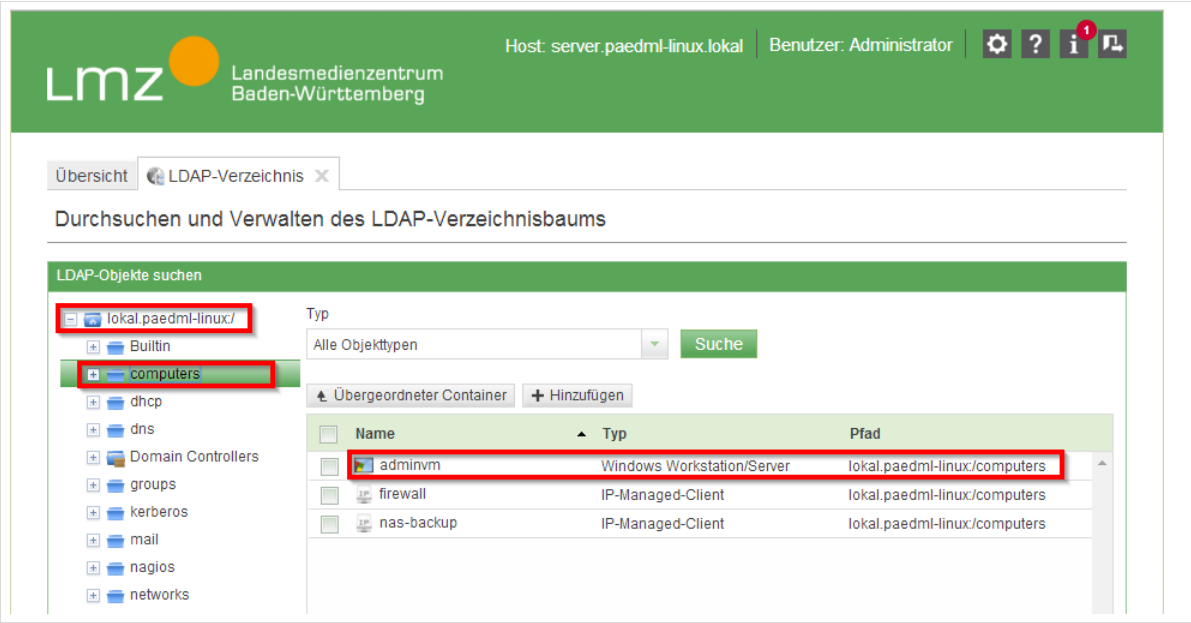


Abb. 197: Kontrolle: Das Objekt „adminvm“ wurde korrekt im LDAP-Baum verschoben.

6.8 Ändern der Proxy-Einstellungen auf der AdminVM

Hintergrund

Für „normale“ Clients ist der **direkte** Internetzugang gesperrt und wird über einen Proxy-Server geleitet, gegenüber dem sich jeder Benutzer authentifizieren muss. Diese Art des Internetzugangs ist auf allen per *opsi* ausgerollten Clients – also auch auf der *AdminVM* – eingestellt. Auf der *AdminVM* laufen jedoch bestimmte Dienste, die eine direkte Internetverbindung benötigen (z.B. *VAMT*).

Die Firewall ist im Auslieferungszustand so konfiguriert, dass der Client *AdminVM*[4] ohne Proxyserver ins Internet darf. Somit ist nur noch die Proxykonfiguration der Maschine lokal anzupassen.

Die Browser *Internet Explorer* und *Chrome* lesen die Proxyeinstellung aus den *Windows*-Einstellungen aus, wohingegen andere Browser (z.B. *Mozilla Firefox*) eigene Proxyeinstellungen haben.

Vorgehensweise

Öffnen Sie die Systemsteuerung der AdminVM und klicken sie auf „*Internetoptionen*“:

[4] Die Firewall Regel betrifft genau gesagt die IP-Adresse 10.1.0.13.Dies ist auch einer der Gründe, warum die AdminVM genau diese IP-Adresse bekommen muss.

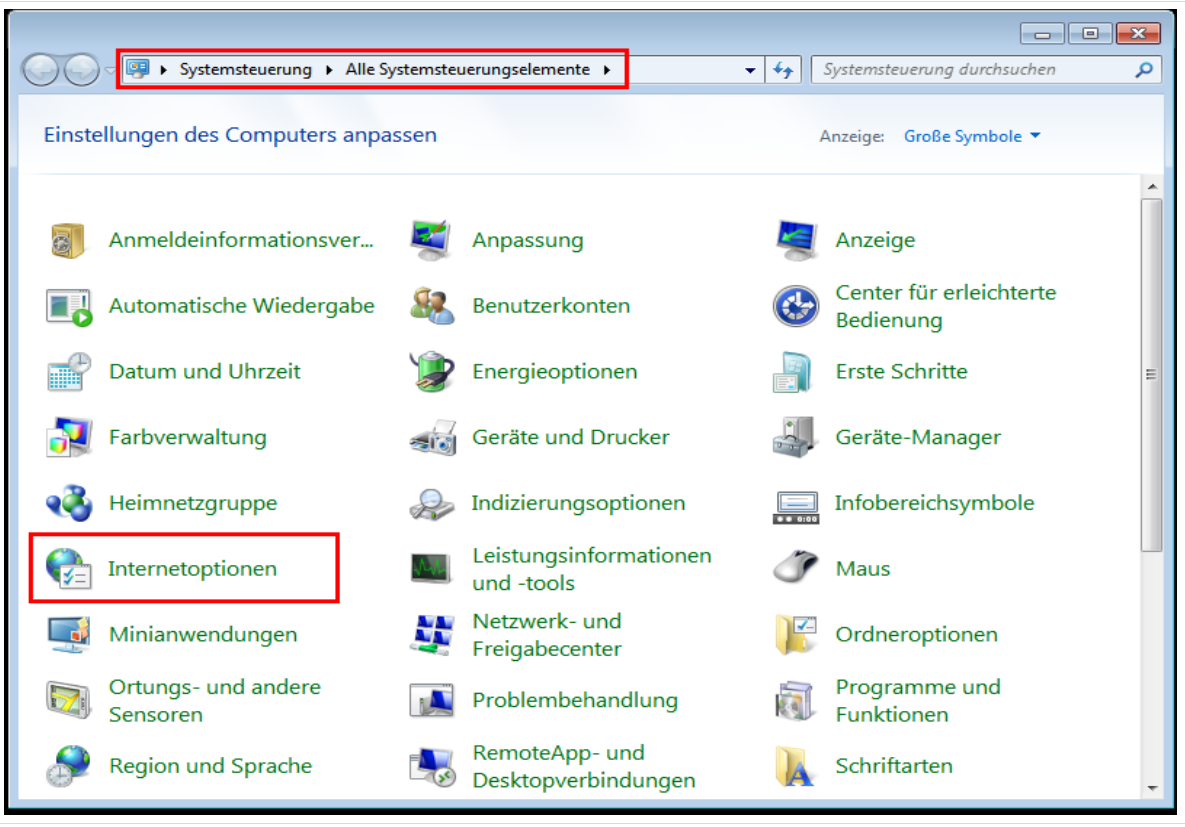


Abb. 198: Systemsteuerung | Internetoptionen

Wählen sie im Fenster „*Eigenschaften von Internet*“ den Reiter „*Verbindungen*“ aus und klicken Sie auf „*LAN-Einstellungen*“:

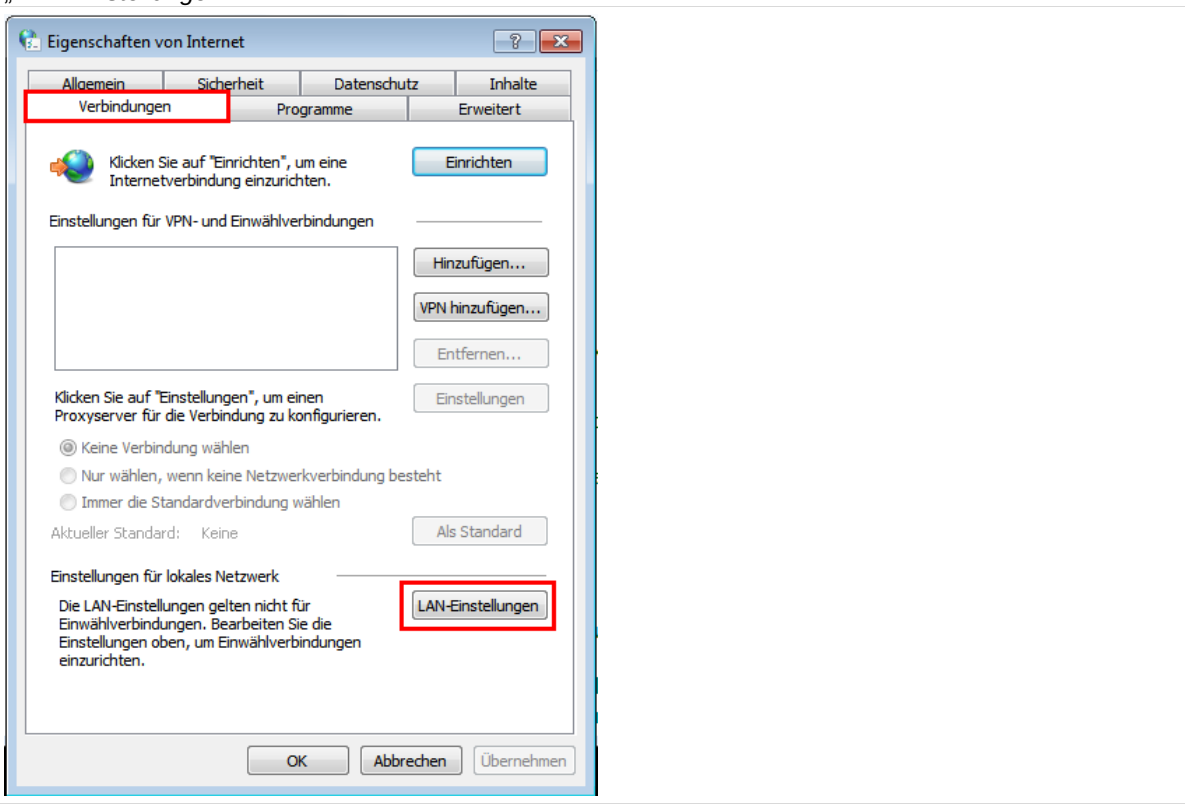


Abb. 199: Verändern der LAN-Einstellungen

Entfernen Sie im folgenden Fenster den Haken bei „*Automatische Suche der Einstellungen*“. Kontrollieren Sie, ob auch der Haken bei „*Proxyserver für LAN verwenden*“ deaktiviert ist. Bestätigen Sie dann mit „*OK*“.

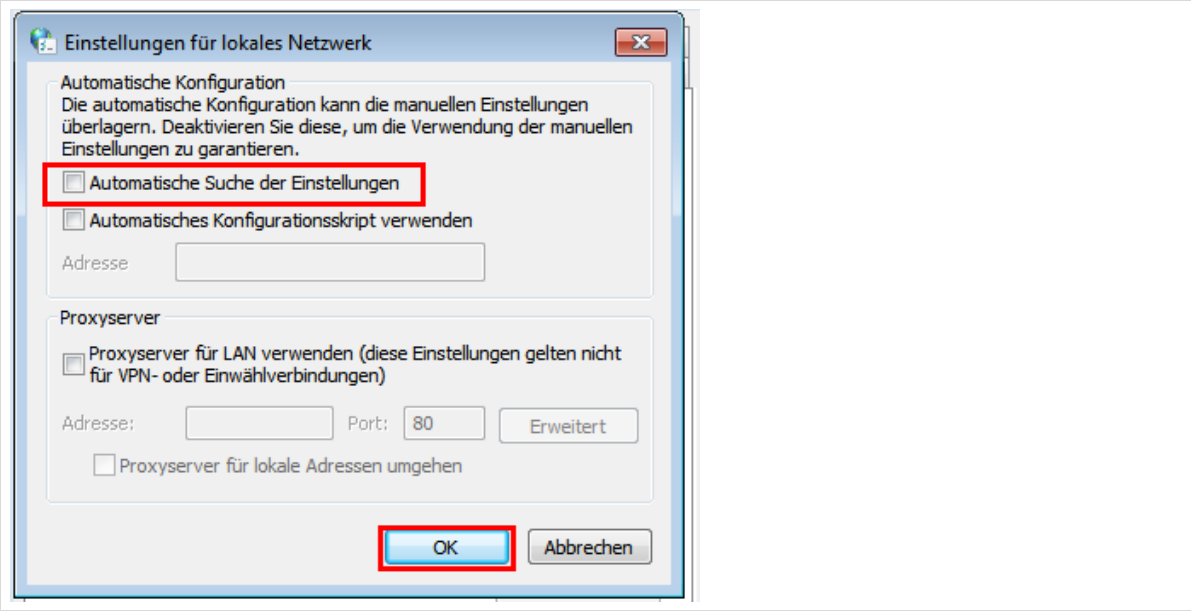


Abb. 200: Entfernen des Hakens bei „Automatische Suche der Einstellungen“

Danach gelangen Sie wieder ins vorige Fenster, das Sie mit „*OK*“ schließen können, Die Systemsteuerung kann ebenfalls geschlossen werden.

6.9 RDP-Zugriff auf die AdminVM

Es gibt mehrere technische Möglichkeiten, um auf die AdminVM zuzugreifen

- per vSphere-Client
- per Remote Desktop Protocol (RDP)
- per Software von Drittanbietern (z.B. TeamViewer, VNC etc.)

Da RDP standardmäßig auf jedem *Windows*-Rechner installiert ist, empfehlen wir diesen Weg.

6.9.1 Einrichten der AdminVM für den RDP-Zugriff

Öffnen Sie auf der AdminVM die Systemeinstellungen durch eine der folgenden Methoden:

- Rechtsklick auf das „*Computer*“-Symbol auf dem Desktop (falls vorhanden), dann „Eigenschaften“
- Klick auf „*Start* | *Einstellungen* | *Systemsteuerung* | *System*“
- Drücken der Tasten Windows + Pause

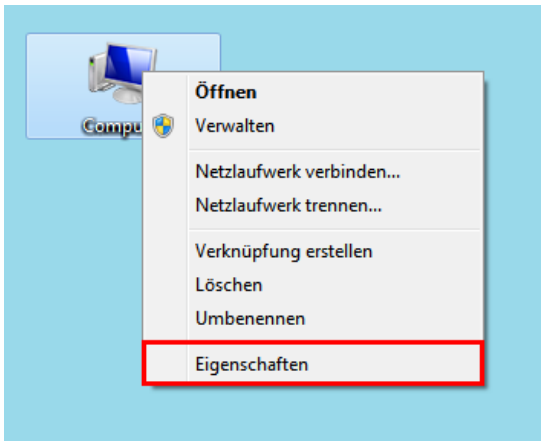


Abb. 201: Öffnen der Systemeinstellungen

Klicken Sie im folgenden Fenster auf „*Remoteeinstellungen*“:

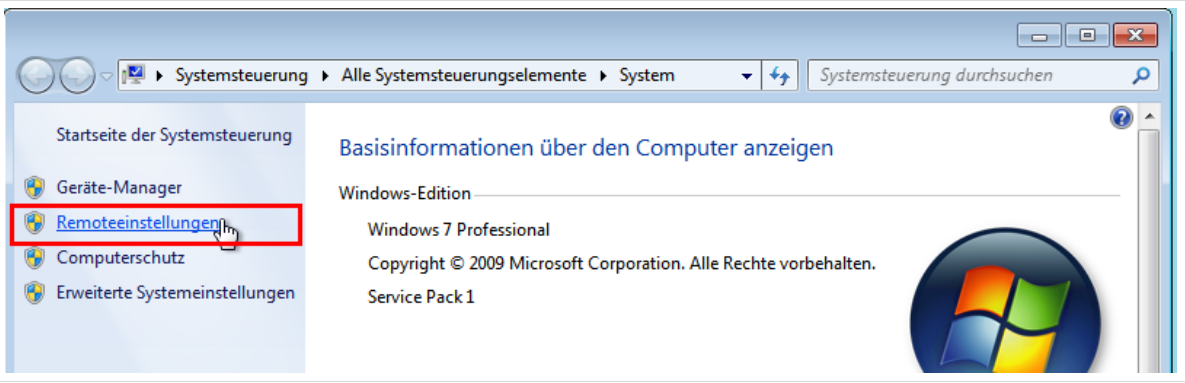


Abb. 202: Konfigurieren der Remoteeinstellungen

Wählen Sie den Reiter „*Remote“* aus. Setzen Sie den Haken bei „*Remoteunterstützungsverbindung mit diesem Computer zulassen*“. Wählen sie im Bereich „*Remotedesktop*“ die zweite Option „*Verbindungen von Computern zulassen…*“, wie im Screenshot gezeigt.

Klicken Sie anschließend auf „*Benutzer auswählen…*“, um diejenigen Benutzer auszuwählen, die per RDP auf die AdminVM zugreifen dürfen.

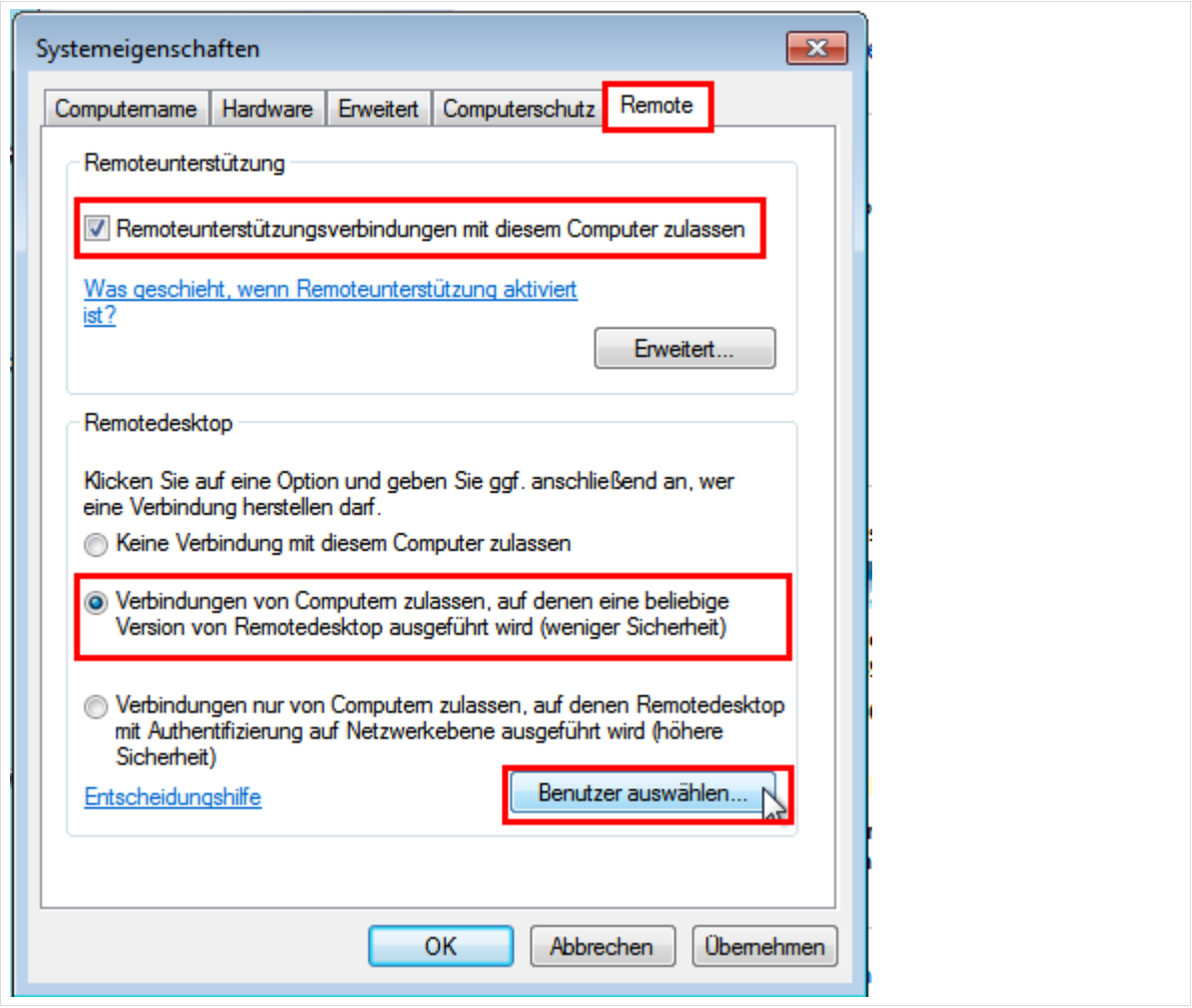

Systemeigenschaften
Computername
Hardware
Erweitert
Computerschutz
Remote
Remoteunterstützung
Remoteunterstützungsverbindungen mit diesem Computer zulassen
Was geschieht, wenn Remoteunterstützung aktiviert ist?
Erweitert...
Remotedesktop
Klicken Sie auf eine Option und geben Sie ggf. anschließend an, wer eine Verbindung herstellen darf.
Keine Verbindung mit diesem Computer zulassen
Verbindungen von Computern zulassen, auf denen eine beliebige Version von Remotedesktop ausgeführt wird (weniger Sicherheit)
Verbindungen nur von Computern zulassen, auf denen Remotedesktop mit Authentifizierung auf Netzwerkebene ausgeführt wird (höhere Sicherheit)
Entscheidungshilfe
Benutzer auswählen...
OK
Abbrechen
Übernehmen

Abb. 203: Einrichten des RDP-Zugriffs auf die AdminVM

Klicken Sie im nächsten Fenster auf „*Hinzufügen*…“.

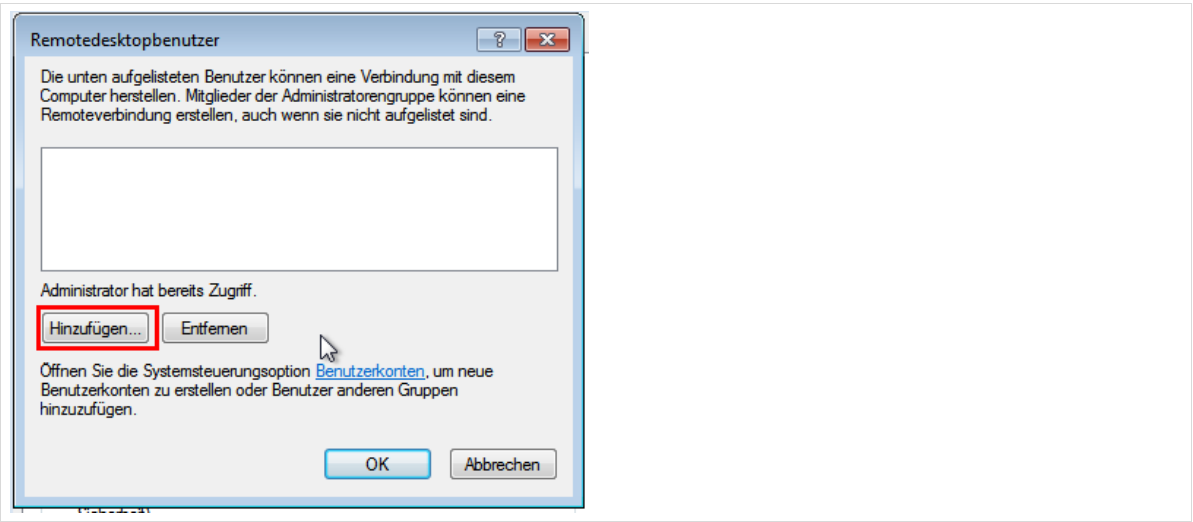

Remotedesktopbenutzer
Die unten aufgelisteten Benutzer können eine Verbindung mit diesem Computer herstellen. Mitglieder der Administratorengruppe können eine Remoteverbindung erstellen, auch wenn sie nicht aufgelistet sind.
Administrator hat bereits Zugriff.
Hinzufügen...
Entfernen
Öffnen Sie die Systemsteuerungsoption Benutzerkonten, um neue Benutzerkonten zu erstellen oder Benutzer anderen Gruppen hinzuzufügen.
OK
Abbrechen

Abb. 204: Hinzufügen eines Benutzers für den RDP-Zugriff

Tragen Sie den Benutzer `Administrator@paedml-linux.lokal` in das angegebene Feld ein und klicken Sie auf „*Namen überprüfen*“:

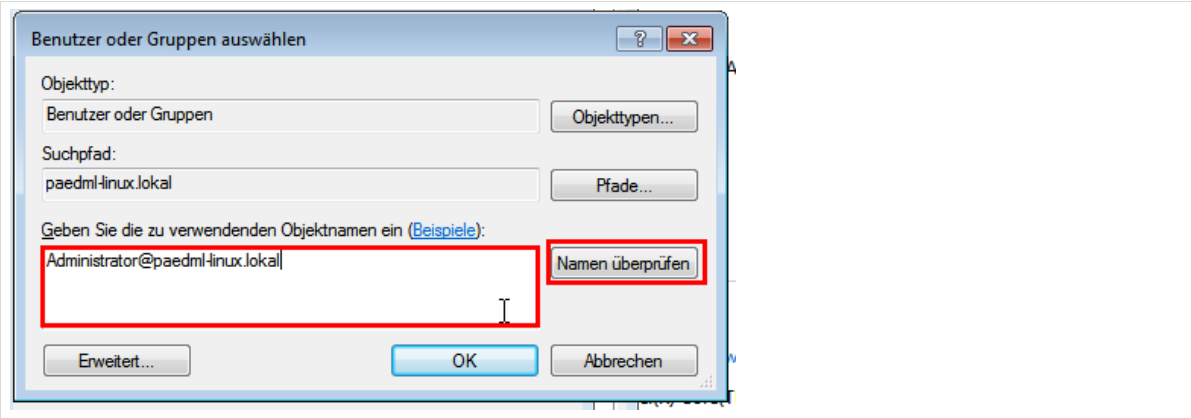


Abb. 205: Eintragen des Benutzers

Im nächsten Fenster müssen Sie sich gegenüber dem Domänencontroller authentifizieren, um die Liste aller Benutzer überprüfen zu dürfen. Tragen Sie dort die Zugangsdaten für den (Domänen-) *Administrator* ein.

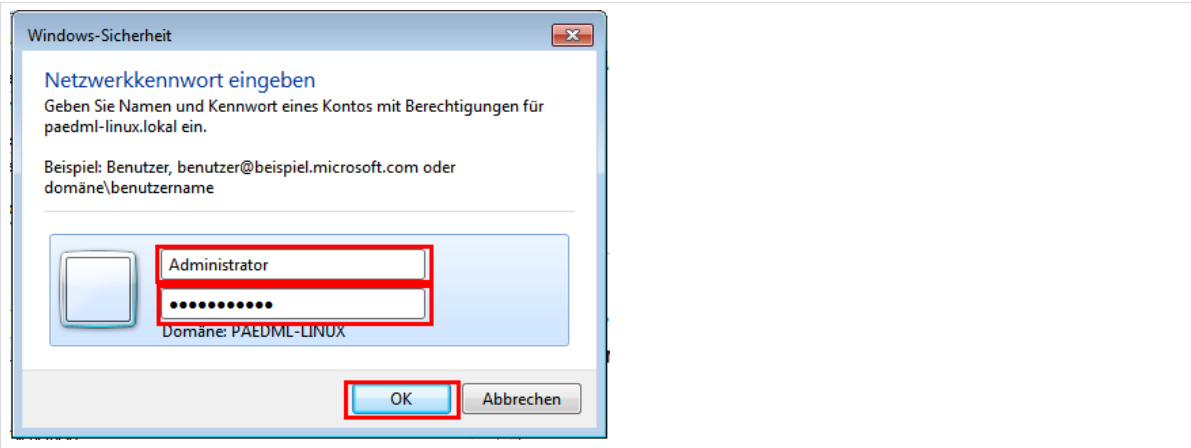


Abb. 206: Authentifizierung als Administrator mit Kennwort

Nach erfolgreicher Authentifizierung wird der soeben eingegebene Benutzer mit dem Domänencontroller abgeglichen und in leicht veränderter Form angezeigt. Klicken Sie auf „*OK*“.

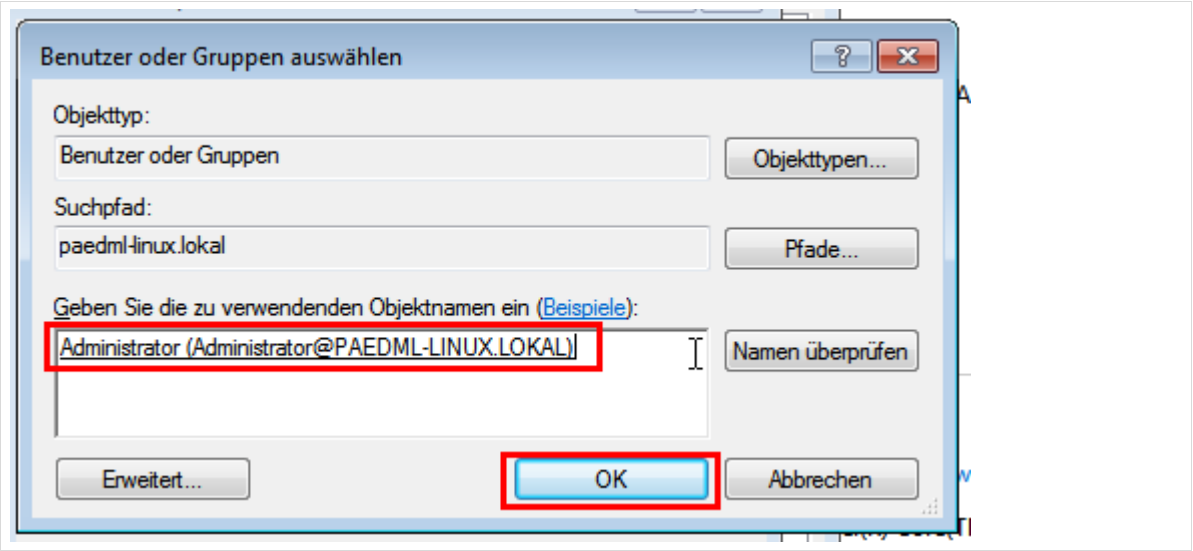


Abb. 207: Der Name wurde erfolgreich überprüft.

Nun ist der Benutzer „Administrator“ berechtigt, eine RDP-Verbindung herzustellen. Klicken Sie erneut auf „*OK*“

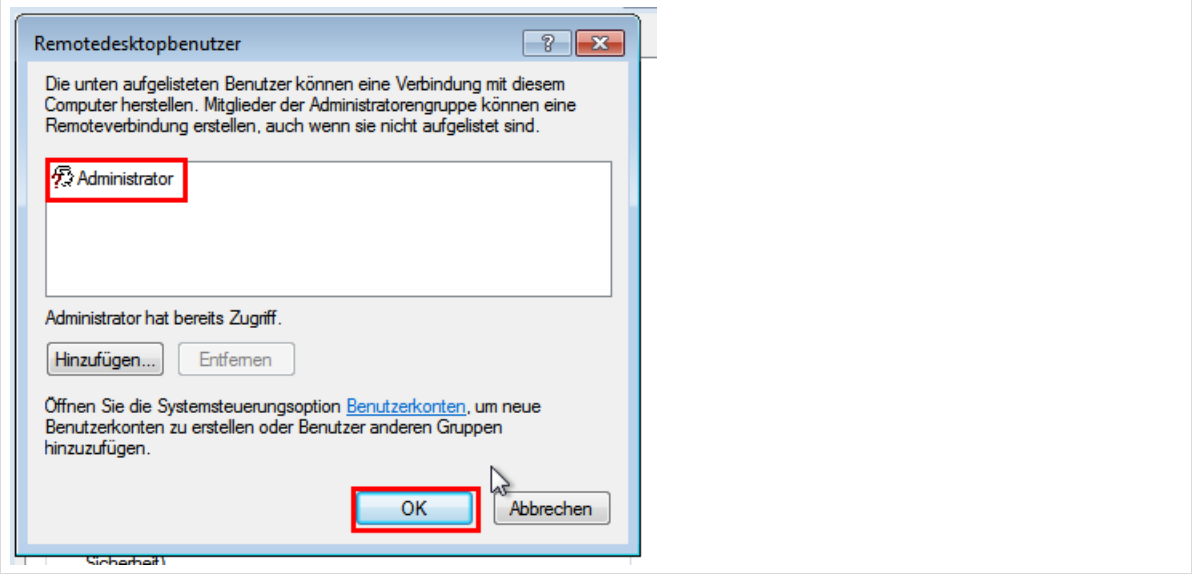

Remotedesktopbenutzer
Die unten aufgelisteten Benutzer können eine Verbindung mit diesem Computer herstellen. Mitglieder der Administratorengruppe können eine Remoteverbindung erstellen, auch wenn sie nicht aufgelistet sind.
Administrator
Administrator hat bereits Zugriff.
Hinzufügen...
Entfernen
Öffnen Sie die Systemsteuerungsoption Benutzerkonten, um neue Benutzerkonten zu erstellen oder Benutzer anderen Gruppen hinzuzufügen.
OK
Abbrechen

Abb. 208: Der Benutzer „Administrator“ darf nun per RDP auf die AdminVM zugreifen.

Sie können die Systemeigenschaften der AdminVM nun mit „*OK*“ schließen.

Damit ist der Zugriff auf die AdminVM per RDP eingerichtet.

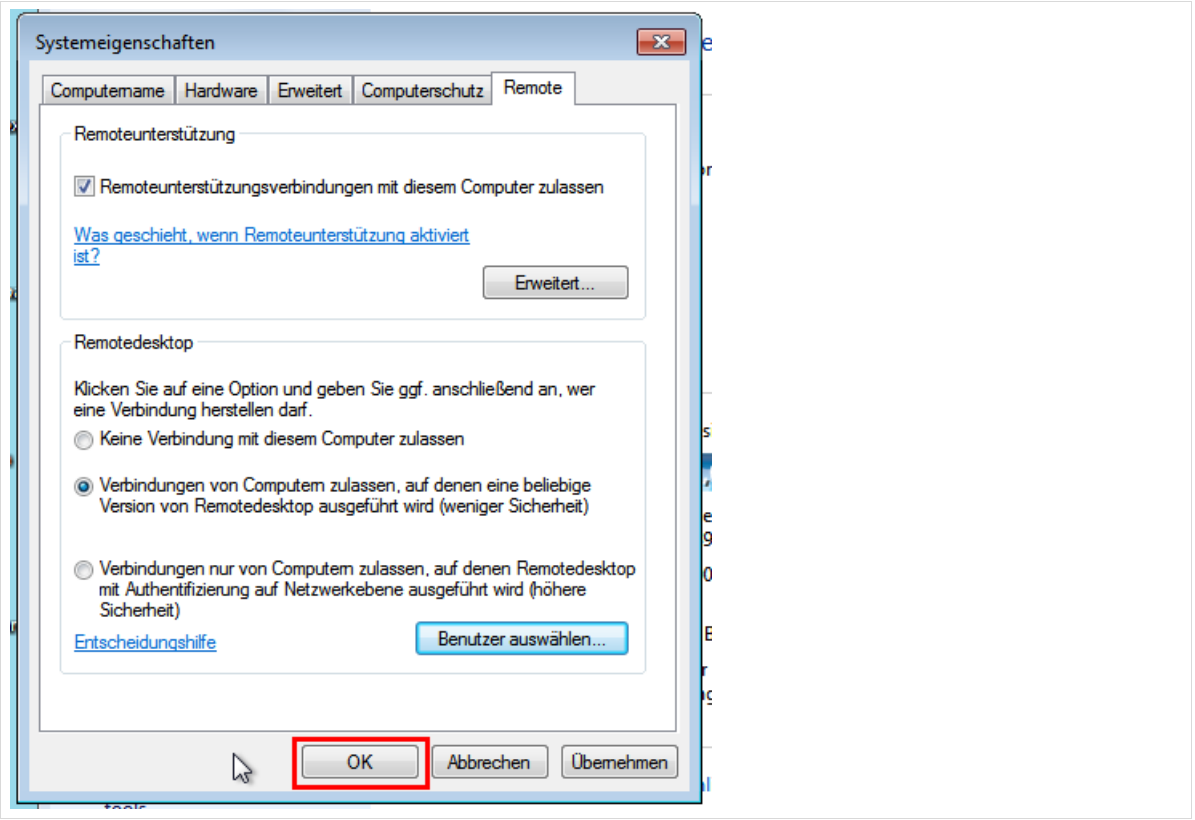

Systemeigenschaften
Computername
Hardware
Erweitert
Computerschutz
Remote
Remoteunterstützung
Remoteunterstützungsverbindungen mit diesem Computer zulassen
Was geschieht, wenn Remoteunterstützung aktiviert ist?
Erweitert...
Remotedesktop
Klicken Sie auf eine Option und geben Sie ggf. anschließend an, wer eine Verbindung herstellen darf.
Keine Verbindung mit diesem Computer zulassen
Verbindungen von Computern zulassen, auf denen eine beliebige Version von Remotedesktop ausgeführt wird (weniger Sicherheit)
Verbindungen nur von Computern zulassen, auf denen Remotedesktop mit Authentifizierung auf Netzwerkebene ausgeführt wird (höhere Sicherheit)
Entscheidungshilfe
Benutzer auswählen...
OK
Abbrechen
Übernehmen

Abb. 209: Schließen der Systemeigenschaften

6.9.2 Test des Zugriffs per RDP auf die AdminVM

Dieser Schritt ist nicht Teil der Installation. Er kann auch zu einem späteren Zeitpunkt von jedem *Windows*-Rechner im Schul-Netz ausgeführt werden.

Öffnen Sie von demjenigen Rechner, von dem Sie auf die AdminVM zugreifen wollen, die Remotedesktopverbindung über „*Start* | *Programme* | *Zubehör* | *Remotedesktopverbindung*“:

Abb. 210: Startmenü | Programme | Zubehör | Remotedesktopverbindung

Tragen Sie im Feld „*Computer*“ den Wert *adminvm.paedml-linux.lokal* ein. Sollte dies aufgrund der DNS-Konfiguration fehlschlagen, können Sie alternativ die IP-Adresse *10.1.0.13* eintragen.

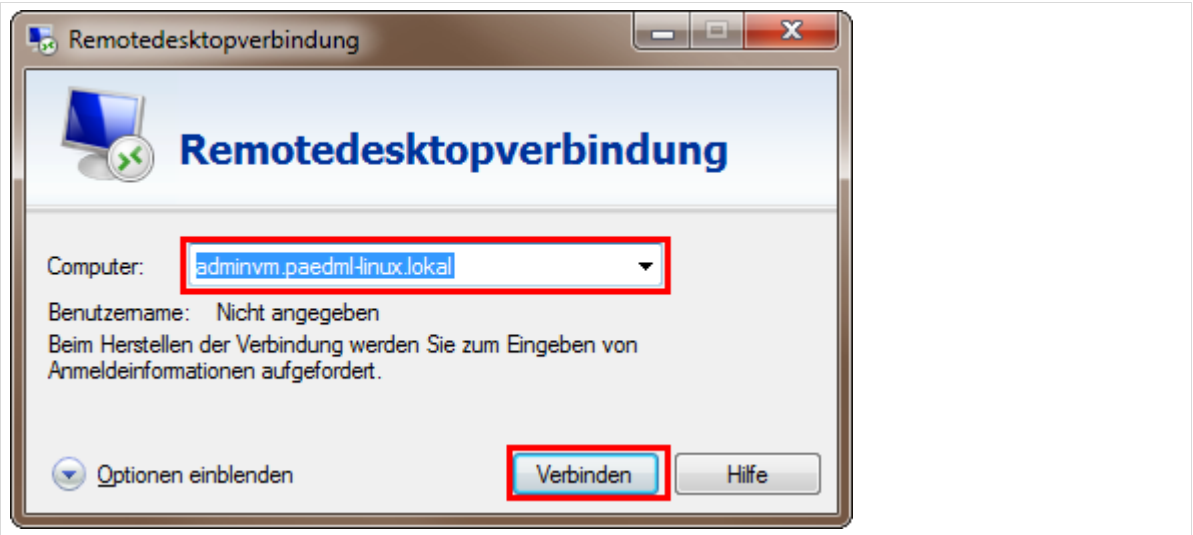


Abb. 211: Aufbau einer Remotedesktopverbindung zur AdminVM

Nun müssen Sie sich an der *AdminVM* authentifizieren. Geben Sie dazu den Benutzernamen *Administrator* (=Domänenadministrator) und das zugehörige Kennwort ein:

Wir empfehlen ausdrücklich, die **Anmeldedaten nicht zu speichern** (Haken nicht setzen!).

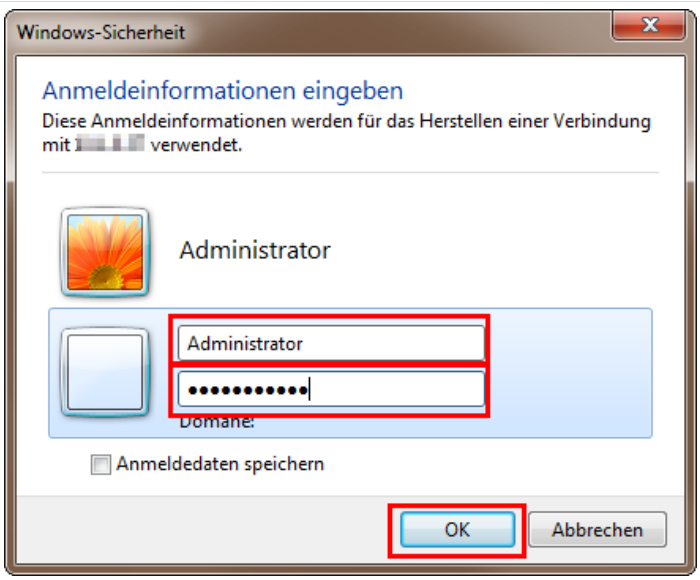


Abb. 212: Anmeldung an der AdminVM

Daraufhin sollte der Desktop der AdminVM in einem Fenster angezeigt werden und Sie können an diesem Rechner arbeiten. Sie beenden die RDP-Sitzung einfach, indem Sie das Fenster schließen.

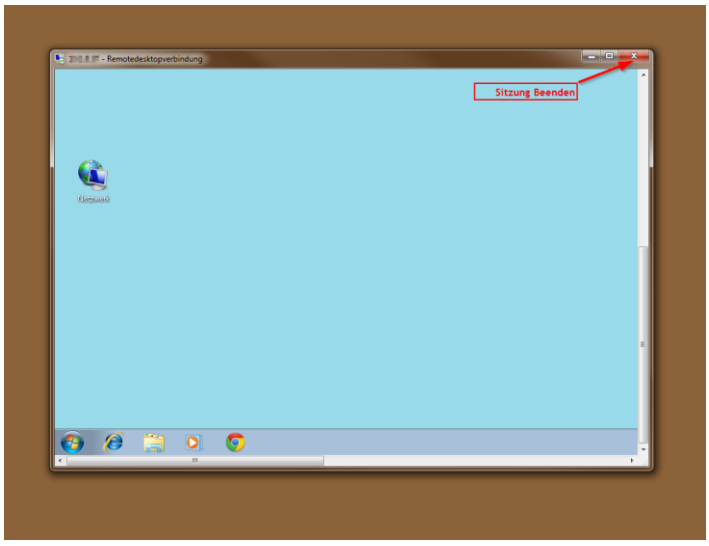


Abb. 213: Zugriff per RDP auf die AdminVM

7. Automatischer Start der virtuellen Maschinen

Die hier beschriebenen Schritte für den automatischen Start virtueller Maschinen sollten **UNBEDINGT** ausgeführt werden.

Nur so kann der Server zum Beispiel im Falle eines Stromausfalles ohne Eingriff von außen wieder gestartet werden.

VMware bietet die Möglichkeit, dass virtuelle Maschinen beim Start des Hypervisors automatisch gestartet werden. Dies kann und sollte für den Fall, dass der Server ausgeschaltet wird, eingerichtet werden.

Beispiel-Szenario:
Ein Bagger hat bei Bauarbeiten ein Stromkabel beschädigt, über das die Schule mit Strom versorgt wird. Der Schaden wurde repariert und das Schulnetz soll wieder in Betrieb genommen werden. Der Schulserver (Hypervisor) wird wieder angeschaltet und (im Idealfall) ca. eine Viertelstunde später kann der IT-Betrieb der Schule wieder aufgenommen werden, da die virtuellen Maschinen beim Start des Servers gestartet werden.

Sofern der Autostart nicht konfiguriert wurde, müssen die virtuellen Maschinen von Hand gestartet werden. Dies kann über den *Management-PC* geschehen. Im „schlimmsten Fall“ muss der Dienstleister vor Ort kommen und diese Aufgaben durchführen.

7.1 Einrichtung des automatischen Starts

1. Öffnen Sie den *vSphere-Client* und melden Sie sich mit Ihren Zugangsdaten an.
2. Wählen Sie in der Bestandsliste die IP-Adresse, bzw. den Hostnamen des *ESXi* Servers aus (1).
3. Wählen Sie den Reiter „*Konfiguration*“ (2).
4. Im Abschnitt "*Software*" wählen Sie den Punkt "*VM starten/herunterfahren*" (3) aus.
5. Dort klicken Sie auf "*Eigenschaften*" (4). Es öffnet sich ein neues Fenster.

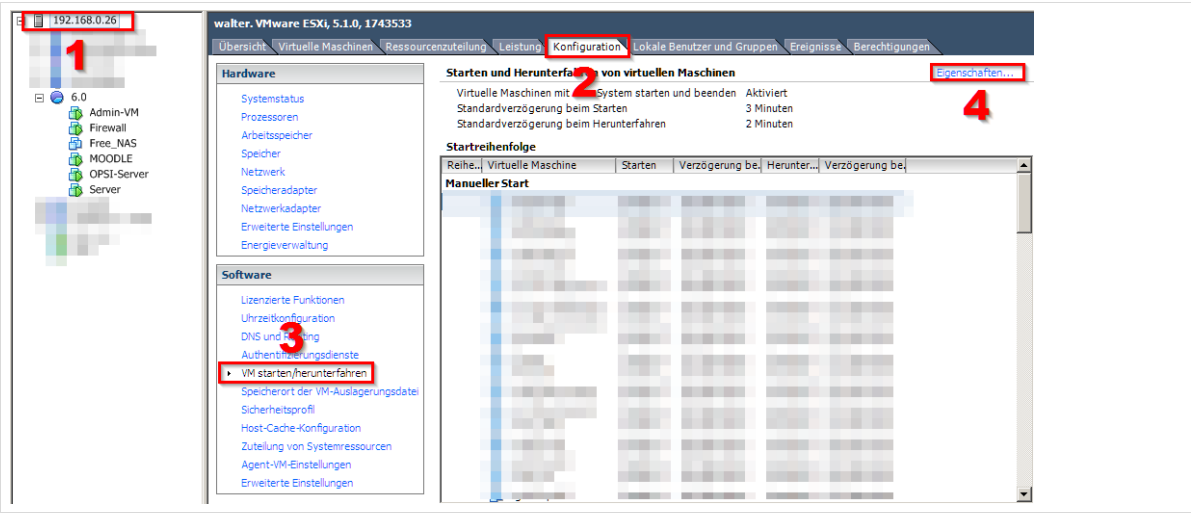


Abb. 214: Konfiguration von automatischem Start der virtuellen Maschinen

6. Hier aktivieren Sie den Haken vor der Checkbox "*Automatisches Starten und Herunterfahren von virtuellen Maschinen zulassen*" (5). **Das automatische Starten und Herunterfahren setzt voraus, dass auf den virtuellen Maschinen „VMware-Tools“ installiert sind.**
7. Wählen Sie im entsprechenden Dropdown-Menü (6) den Eintrag „*Herunterfahren des Gastes*“ aus.
8. Abschließend muss die Startreihenfolge der Clients festgelegt werden. Wechseln Sie hierfür in das Feld „*Startreihenfolge*“ (7) und wählen Sie den automatisch zu startenden Rechner aus. Mit den Tasten „*Nach oben*“ und „*Nach unten*“ können Sie die Position der Rechner in der Liste ändern. Wiederholen Sie den Vorgang für alle automatisch zu startenden Rechner. Die folgende Startreihenfolge muss eingestellt werden:
   - Firewall
   - Server
   - opsi-Server
   - AdminVM
   - (optional:) weitere Server, sofern eingerichtet.

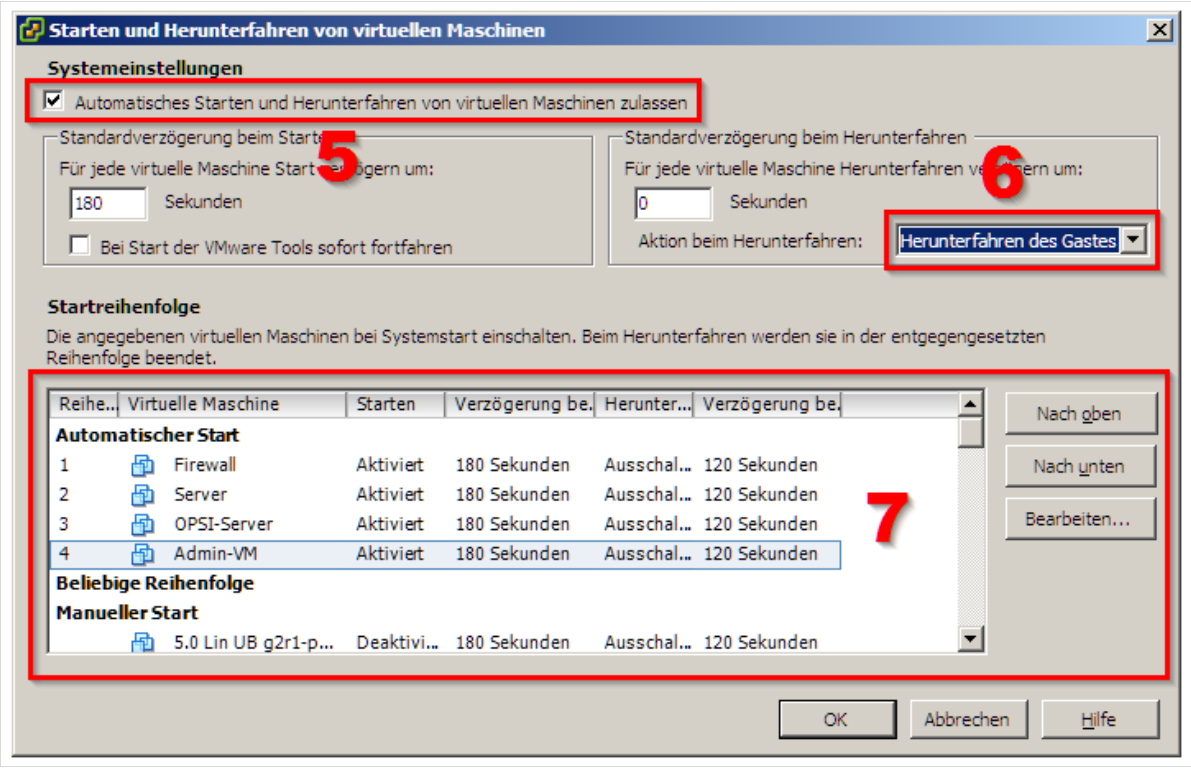


Abb. 215: Konfiguration von automatischem Start der virtuellen Maschinen

8. Rahmenbedingungen für die Backuplösung

8.1 Grundsätzliches zum Betrieb einer NAS

Die Datensicherung der *paedML Linux* erfolgt mit Hilfe von *BackupPC*. Der Umgang mit *BackupPC* ist im Administrationshandbuch beschrieben. Dort finden sich auch Überlegungen zu den Hardwareanforderungen einer NAS. An dieser Stelle wird nur auf die Netzwerkschicht bzw. die Bereitstellung des Speicherplatzes eingegangen.

Für die Datensicherung via *BackupPC* muss Speicherplatz außerhalb des Virtualisierungs-Hosts bereitgestellt werden. Hierfür ist der Einsatz einer NAS-Lösung („*Network Attached Storage*“) vorgesehen. Da bei Backupvorgängen extrem hohe Datenmengen anfallen, ist darauf zu achten, dass die Netzverbindung (auch der Switch!) zwischen NAS und VM „*Server*“ bzw. dem Virtualisierungs-Host auf großen Datendurchsatz ausgerichtet ist.

8.2 Anbindung der NAS ins Netz

Aufgrund der Vielzahl der am Markt erhältlichen NAS-Lösungen kann an dieser Stelle nur allgemein auf die Verbindung zur NAS eingegangen werden. Die Konfiguration ist abhängig von der eingesetzten Hardware.

Die Einrichtung und Wartung einer NAS ist Aufgabe des Dienstleisters. Die Mitarbeiter der Hotline können nur unterstützend wirken.

Ein NAS-System wird im Netz „*PAEDAGOGIK*“ betrieben, dafür ist die IP-Adresse *10.1.0.12* reserviert. Eine Vorlage für die Maschine wurde am Server eingerichtet. Daher muss das Gerät nur nach den hier gemachten Vorgaben eingerichtet werden, um eine Datensicherung zu gewährleisten.

Parameter	Wert
IP-Adresse	10.1.0.12
Subnetzmaske	255.255.255.0
Hostname:	nas-backup.paedml-linux.lokal
DNS-Server (optional)	10.1.0.1
Gateway (optional)	10.1.0.11

Tabelle 5: IP-Konfiguration der NAS

8.3 NFS-Share einrichten

Die Backupsoftware „*BackupPC*“ legt die Backups standardmäßig im Verzeichnis */mnt/backuppc* ab. Damit die Sicherungen auch wirklich auf der NAS landen, müssen folgende Einstellungen getroffen werden:

- Freigabe eines Verzeichnisses auf der NAS der NFS, auf das von der VM „*Server*“ aus zugegriffen werden kann. Dieses Verzeichnis muss gegen unberechtigten Zugriff geschützt werden. Dies geschieht – abhängig vom Modell der NAS – zum Beispiel, in dem der Zugriff auf bestimmte Benutzer oder auf IP-Adressen beschränkt wird.
- Einrichten eines NFS-Mounts auf dem Server, so dass das Verzeichnis */mnt/backuppc* auf das freigegebene Verzeichnis der NAS zeigt.
- Einstellen der Zugriffsberechtigung auf der NAS, d.h. der Systembenutzer „*root*“ muss Vollzugriff haben.

9. Starten und Stoppen von virtuellen Maschinen

Zum Starten und stoppen der virtuellen Maschinen gibt es mehrere Möglichkeiten, die im Folgenden beschrieben werden.

9.1 Starten von virtuellen Maschinen

Markieren Sie die virtuelle Maschine im Auswahlfenster des vSphere-Clients. Der *vSphere-Client* bietet eine Vielzahl an Möglichkeiten, eine VM einzuschalten, drei Möglichkeiten sind im Folgenden dargestellt:

- Klick auf das Start-Icon in der oberen Menüleiste
- Klick auf "*Einschalten*" im Reiter "*Übersicht*", Bereich "*Befehle*"
- Rechtsklick auf die VM, dann "*Betrieb* | *Einschalten*"

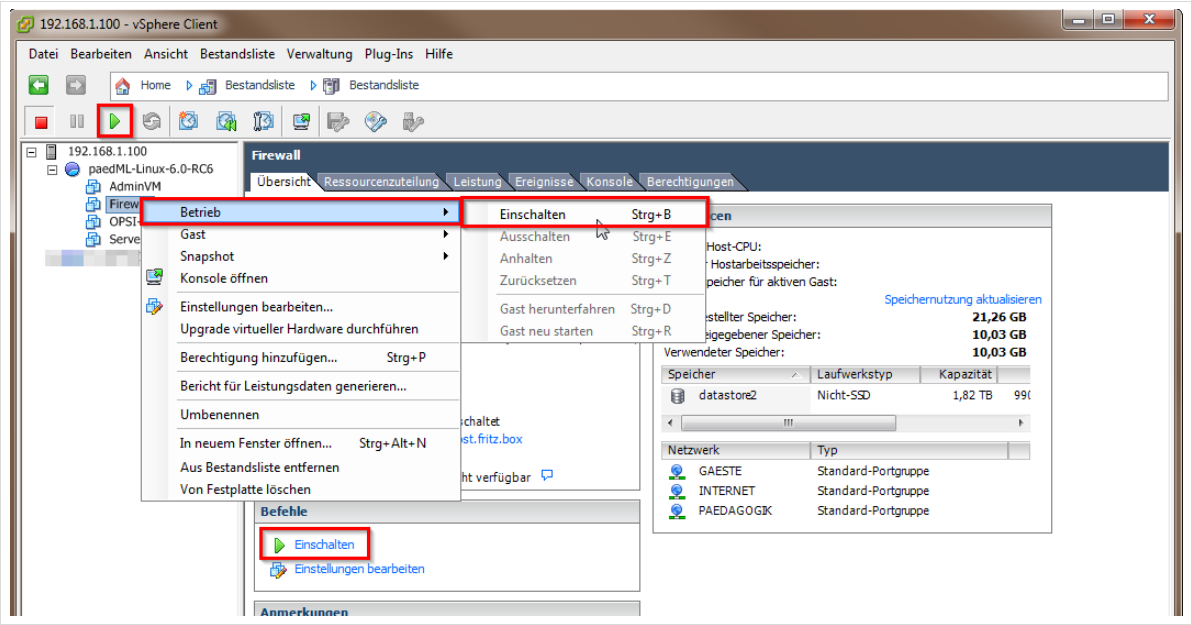


Abb. 216: Möglichkeiten zum Starten einer virtuellen Maschine]

9.2 Startreihenfolge

Starten Sie virtuelle Maschinen immer in der folgenden Reihenfolge. Beobachten Sie den Startvorgang und schalten Sie die nächste VM erst dann ein, wenn die vorherige vollständig hochgefahren ist.

- *Firewall*
- *Server*
- *opsi-Server*
- *AdminVM*

9.3 Herunterfahren und Neustart virtueller Maschinen

Für das sichere Herunterfahren der virtuellen Maschinen gibt es - je nach Betriebssystem- verschiedene Methoden. Welche Methode Sie wählen, hängt vom konkreten Einsatzfall ab. Fahren Sie die Maschinen in umgekehrter Startreihenfolge zurück, d.h.

- *AdminVM*
- *opsi-Server*
- *Server*
- *Firewall*

9.3.1 Herunterfahren über die Konsole des Betriebssystems

Falls sie gerade auf der auszuschaltenden VM arbeiten, (Textkonsole bei Server, *ospi*--Server und Firewall, Grafische Konsole bei *AdminVM*) können Sie die VM direkt von der Konsole aus herunterfahren bzw. neu starten. Die Vorgehensweisen sind dabei unterschiedlich:

9.3.1.1 AdminVM (Windows)

Fahren Sie das virtuelle System über die gewohnte *Windows*-Abmeldung herunter.

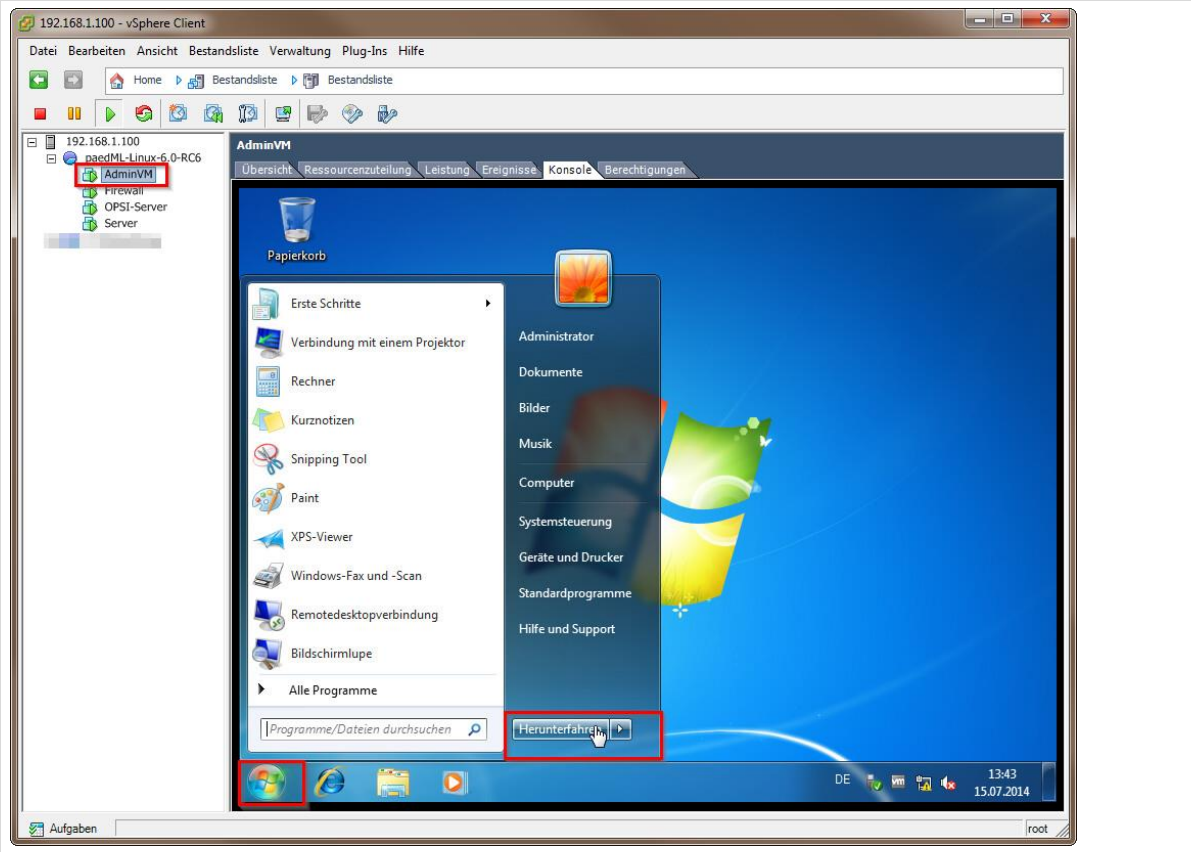


Abb. 217: Normaler Windows Shutdown

9.3.1.2 Server / opsi-Server

Melden Sie sich als Root an der Textkonsole an und führen Sie einen der folgenden Befehle aus:

`# halt` (Maschine herunterfahren)

`# reboot` (Maschine neu starten)

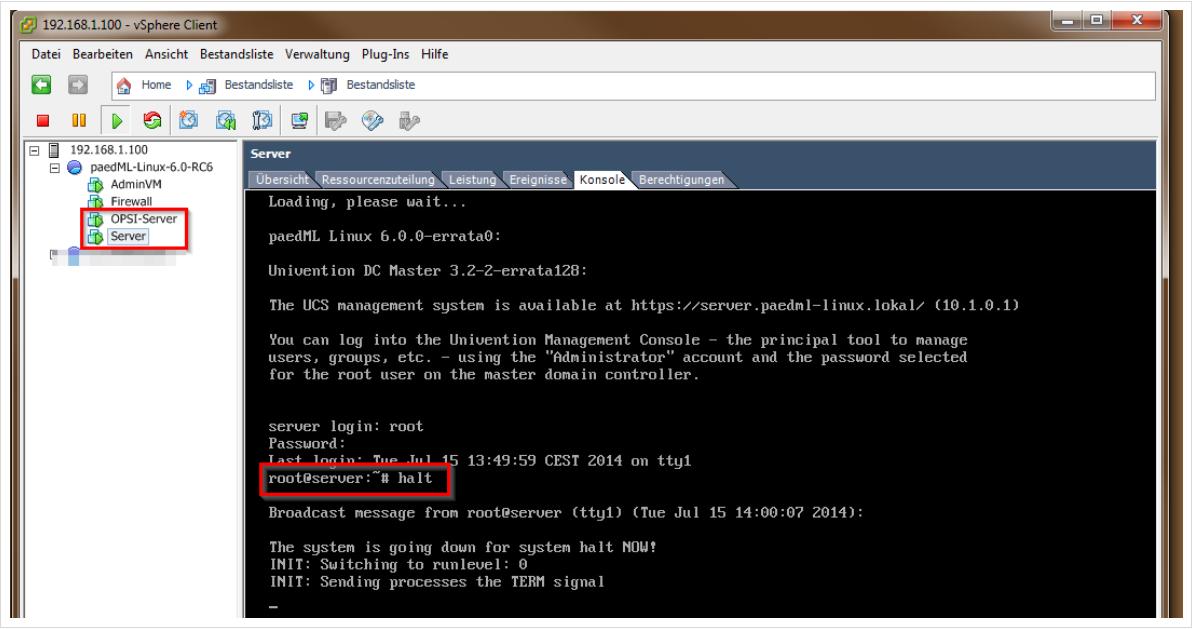

192.168.1.100 - vSphere Client
Datei Bearbeiten Ansicht Bestandsliste Verwaltung Plug-Ins Hilfe
Home Bestandsliste Bestandsliste
192.168.1.100
paedML-Linux-6.0-RC6
AdminVM
Firewall
OPSI-Server
Server
Server
Übersicht Ressourcenzuteilung Leistung Ereignisse Konsole Berechtigungen
Loading, please wait...
paedML Linux 6.0.0-errata0:
Univention DC Master 3.2-2-errata128:
The UCS management system is available at https://server.paedml-linux.lokal/ (10.1.0.1)
You can log into the Univention Management Console - the principal tool to manage
users, groups, etc. - using the "Administrator" account and the password selected
for the root user on the master domain controller.
server login: root
Password:
Last login: Tue Jul 15 13:49:59 CEST 2014 on tty1
root@server:~# halt
Broadcast message from root@server (tty1) (Tue Jul 15 14:00:07 2014):
The system is going down for system halt NOW!
INIT: Switching to runlevel: 0
INIT: Sending processes the TERM signal

Abb. 218: Herunterfahren der VM Server bzw OPSI-Server von der Textkonsole aus]

9.3.1.3 Firewall

Wählen Sie auf der Textkonsole der Firewall die Option "*5) Reboot system*" bzw. "*6) Halt system*" und bestätigen Sie die Auswahl mit "*y*"

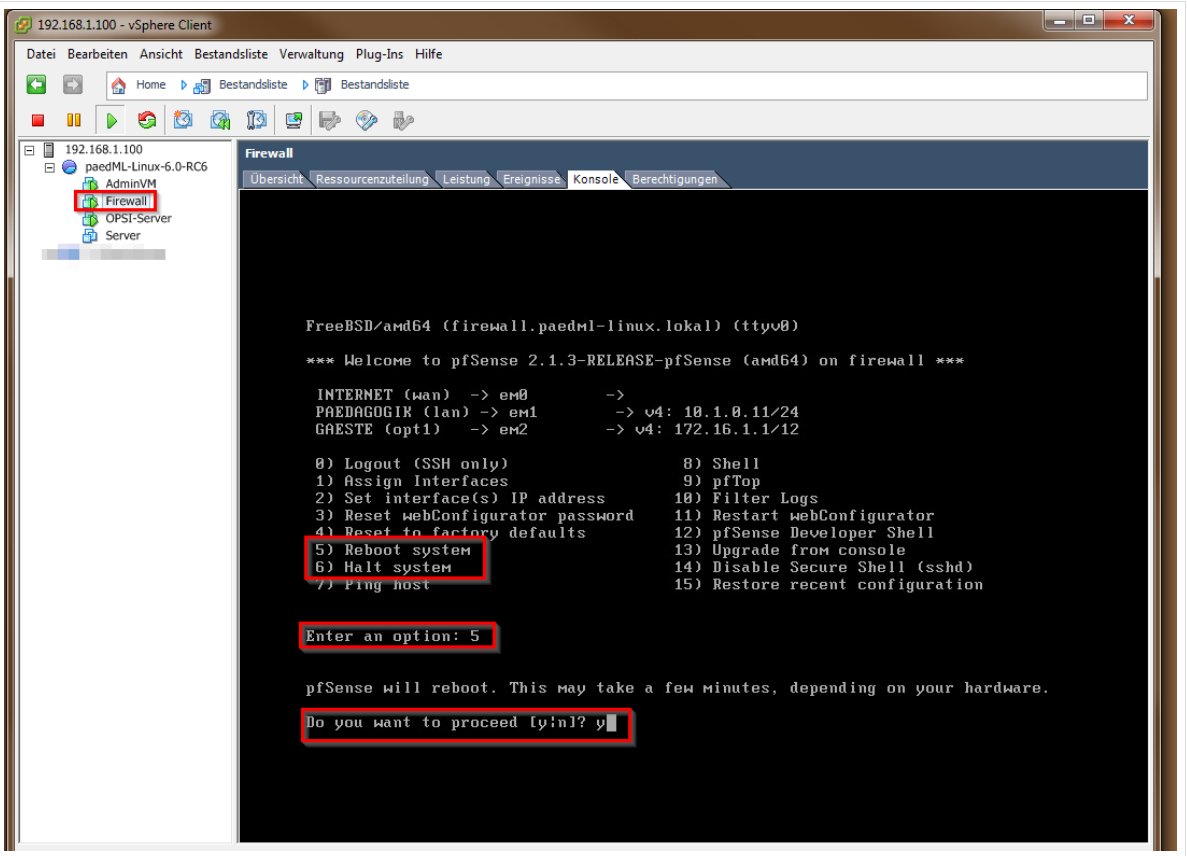

192.168.1.100 - vSphere Client
Datei Bearbeiten Ansicht Bestandsliste Verwaltung Plug-Ins Hilfe
Home Bestandsliste Bestandsliste
192.168.1.100
paedML-Linux-6.0-RC6
AdminVM
Firewall
OPSI-Server
Server
Firewall
Übersicht Ressourcenzuteilung Leistung Ereignisse Konsole Berechtigungen
FreeBSD/amd64 (firewall.paedml-linux.lokal) (ttyv0)
*** Welcome to pfSense 2.1.3-RELEASE-pfSense (amd64) on firewall ***
INTERNET (wan) -> em0 ->
PAEDAGOGIK (lan) -> em1 -> v4: 10.1.0.11/24
GAESTE (opt1) -> em2 -> v4: 172.16.1.1/12
0) Logout (SSH only) 8) Shell
1) Assign Interfaces 9) pfTop
2) Set interface(s) IP address 10) Filter Logs
3) Reset webConfigurator password 11) Restart webConfigurator
4) Reset to factory defaults 12) pfSense Developer Shell
5) Reboot system 13) Upgrade from console
6) Halt system 14) Disable Secure Shell (sshd)
7) Ping host 15) Restore recent configuration
Enter an option: 5
pfSense will reboot. This may take a few minutes, depending on your hardware.
Do you want to proceed [y|n]? y

Abb. 219: Herunterfahren der Firewall von der Textkonsole aus]

9.3.2 Herunterfahren / Neustart durch vSphere-Client

Ein Herunterfahren bzw. ein Neustart kann auch über den *vSphere-Client* ausgelöst werden. Die *VMware-Tools* auf der VM sorgen für das Auslösen eines sicheren Shutdowns. Auf den VM "*Server*", "*opsi-Server*" und "*Firewall*" sind die *VMware-Tools* im Auslieferungszustand bereits installiert, auf der Vm "*AdminVM*" müssen die *VMware-Tools* nachträglich installiert werden. Siehe Kapitel 6.6, Seite 117.

Markieren Sie die VM, klicken Sie auf das "*Stop-Symbol*" in der oberen Menüleiste. Alternative: Rechtsklick auf die VM, dann *"Betrieb | Gast herunterfahren*".

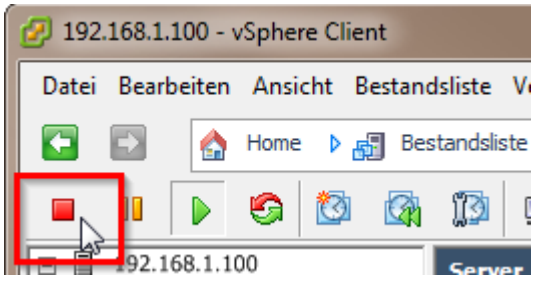


Abb. 220: Gastsystem über Stop-Symbol herunterfahren]

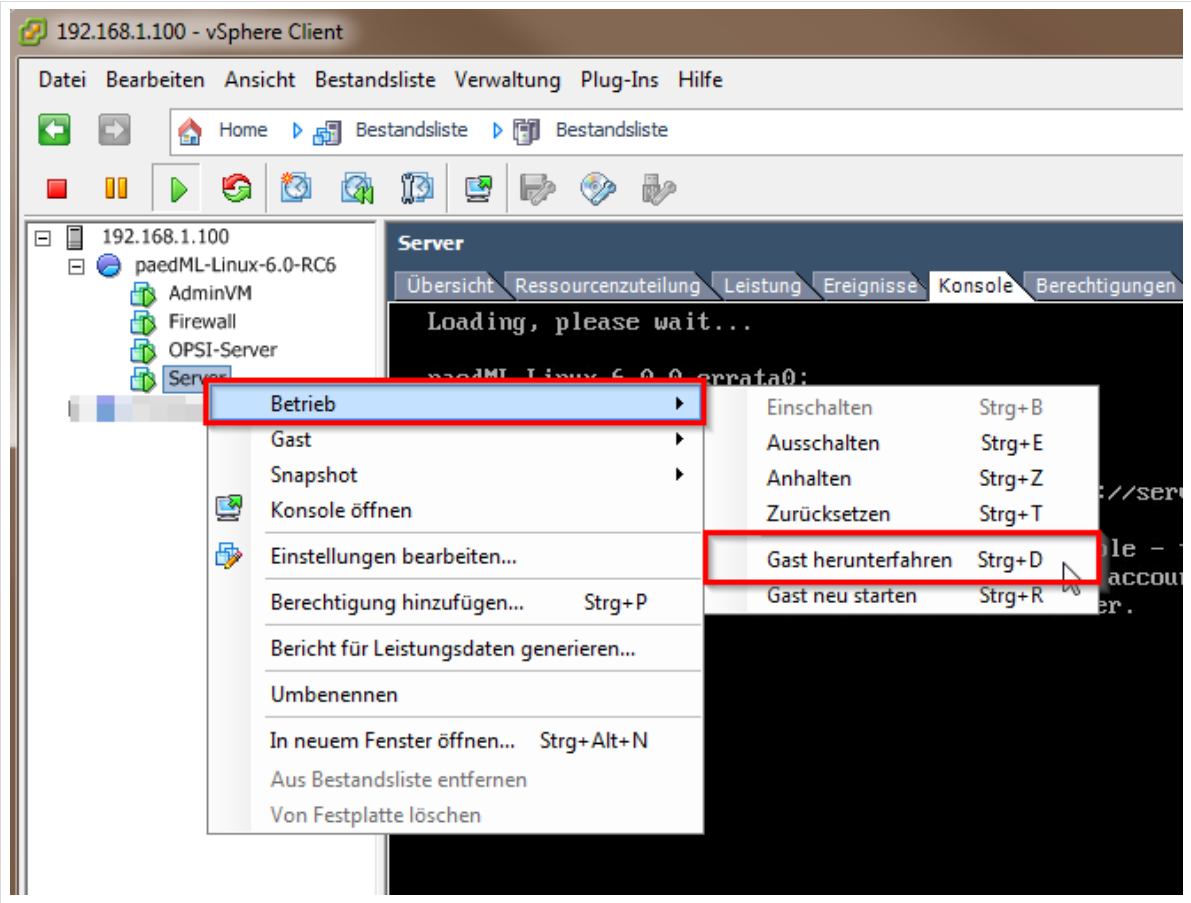


Abb. 221: Gastsystem über Kontextmenü herunterfahren

Für einen Reboot klicken Sie auf das Reboot-Symbol. Alternative: Rechtsklick auf die VM, dann "*Betrieb | Gast neu starten*"

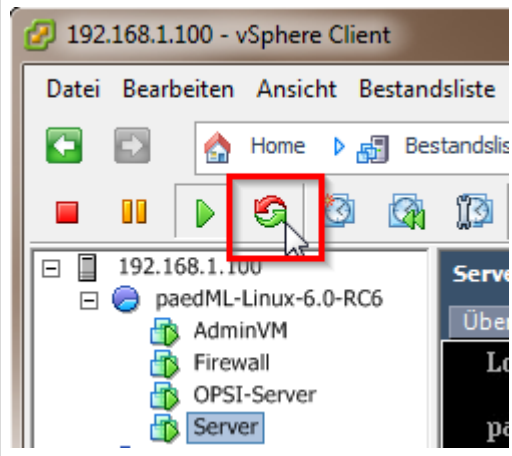


Abb. 222: Gastsystem über Reboot-Symbol neu starten

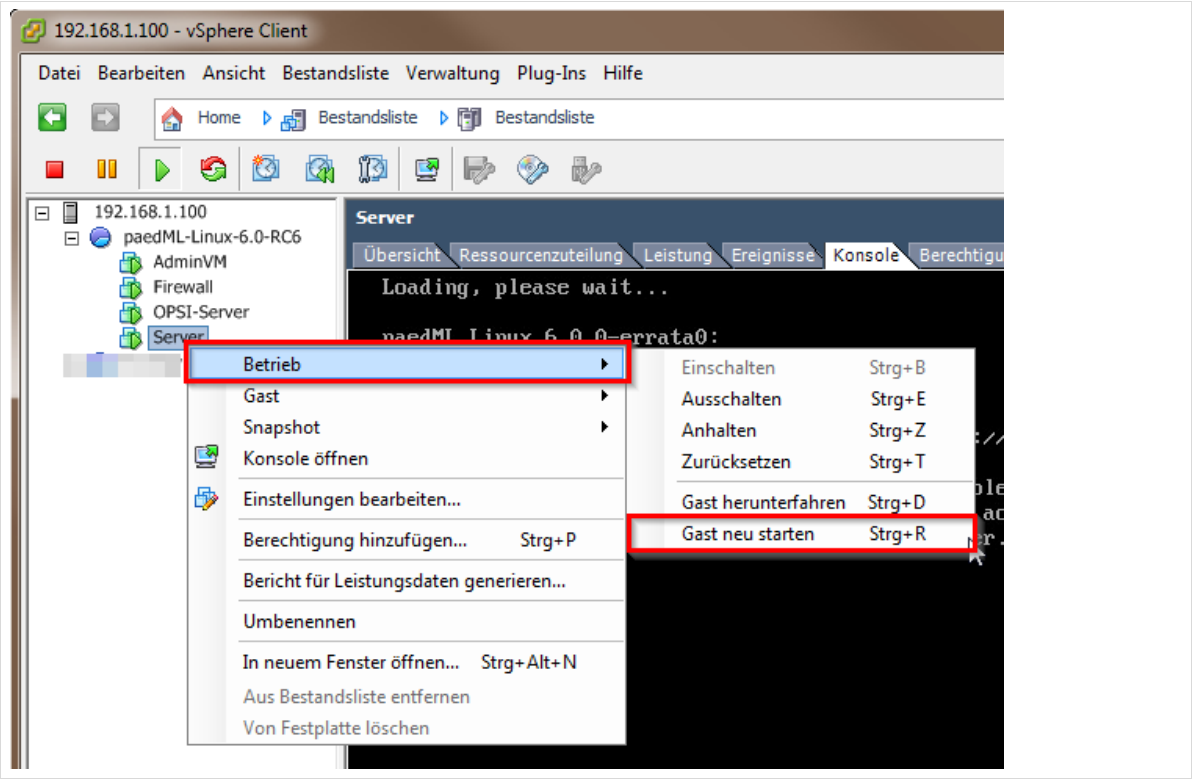


Abb. 223: Gastsystem über Kontextmenü neu starten

9.4 Hartes Ausschalten/ Harter Neustart

Das „harte Ausschalten“ entspricht der Betätigung eines Ein-Ausschalters bzw das Ziehen des Netzsteckers und sollte – wenn irgendwie möglich – vermieden werden! Der einzige Grund, eine VM hart auszuschalten liegt vor, wenn ein sicheres Herunterfahren – z.B. aufgrund eines Systemabsturzes – nicht möglich sein sollte.

Um eine VM hart auszuschalten, klicken Sie mit der rechten Maustaste auf die VM und wählen Sie den Menüpunkt "*Betrieb* | *Ausschalten*" bzw. "*Betrieb* | *Zurücksetzen*"

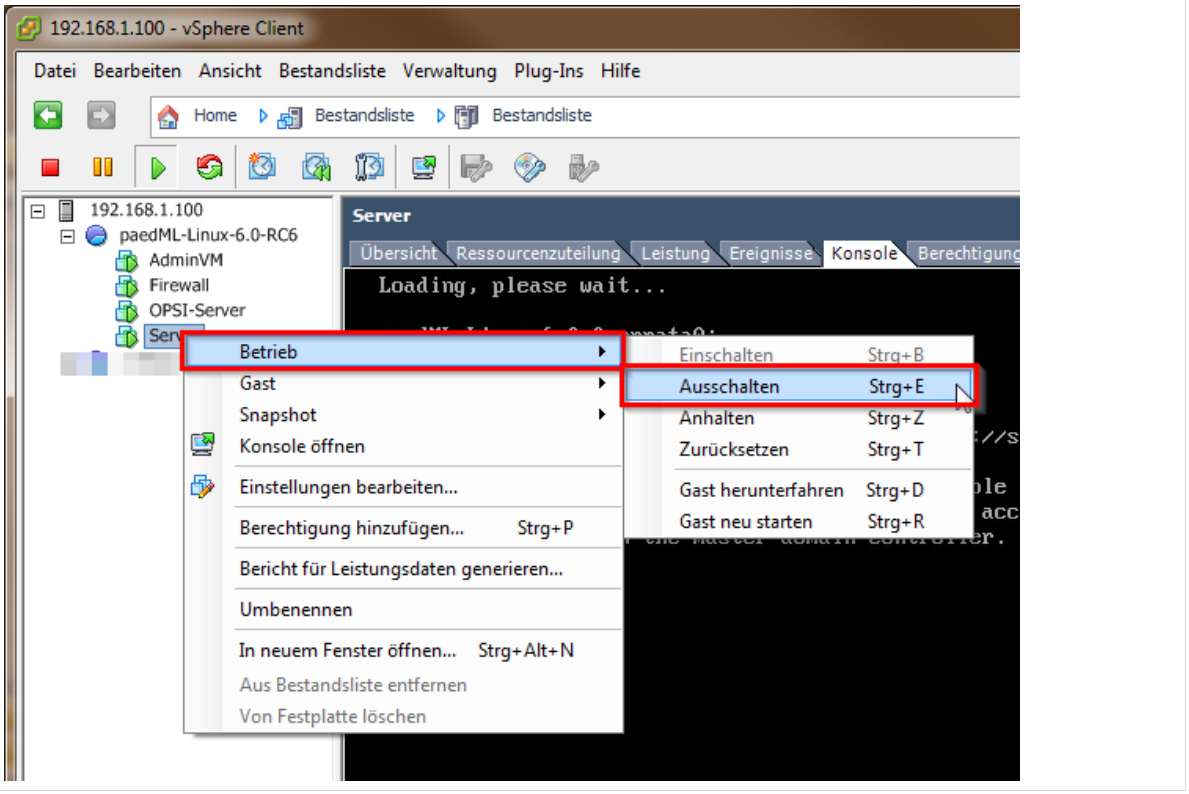


Abb. 224: harter shutdown

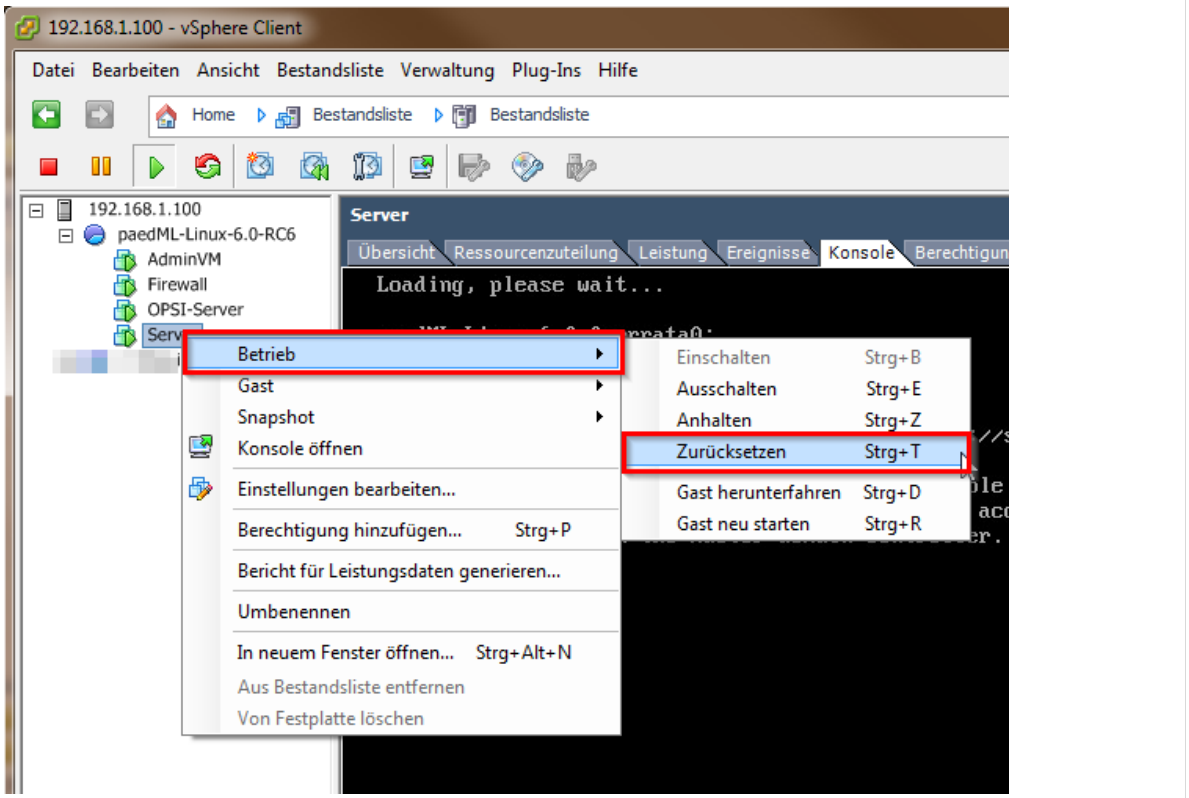


Abb. 225: harter reset

10. Snapshots der virtuellen Maschinen

Der Hypervisor *VMware vSphere ESXi* bietet die Möglichkeit, sogenannte *Snapshots* von virtuellen Maschinen anzufertigen. Dabei handelt es sich um komplette Abbilder der virtuellen Maschinen incl. deren Festplatten.

10.1 Grundsätzliche Informationen zu Snapshots

An dieser Stelle kann die Thematik von Snapshots nicht umfassend behandelt werden, für ein tieferes Verständnis verweisen wir auf die Dokumentation des Hypervisors unter https://www.vmware.com/support/pubs/

Ein Snapshot ist das temporäre Abbild einer virtuellen Maschine. Da die virtuellen Maschinen der *paedML Linux* jedoch eine Einheit bilden, sollten Sie unbedingt beim Erstellen von Snapshots der *paedML Linux* Server folgende Hinweise beachten:

- Die virtuellen Maschinen „*Server*“ und „*opsi-Server*“ müssen immer gemeinsam gesichert und wiederhergestellt werden. Das Sichern oder auch Wiederherstellen nur einer einzelnen virtuellen Maschine kann zu Dateninkonsistenzen und im schlimmsten Fall zu einem nicht mehr lauffähigen *paedML Linux* System führen.
- Snapshots dürfen nur angelegt werden, wenn die virtuellen Maschinen ausgeschaltet sind.
- Das Vorhalten vieler Snapshots kann sich eventuell negativ auf die Performance der virtuellen Maschinen auswirken.
- Ein Snapshot ist **KEIN ERSATZ FÜR EINE DATENSICHERUNG**.

10.2 Erstellen von Snapshots von „Server“ und „opsi-Server“

Herunterfahren der virtuellen Maschinen
Fahren Sie die virtuellen Maschinen „*Server*“ und „*opsi-Server*“ kontrolliert herunter, hierzu gibt es drei Möglichkeiten.

1. **Über vSphere-Client:** Rechtsklick im vSphere-Client auf die entsprechende VM, danach Klick auf „*Betrieb* | *Gast herunterfahren*“.
2. **Über Schulkonsole:** Melden Sie aus einem Browser im Netz „*PAEDAGOGIK*“ (z.B. aus der „*AdminVM*“ als „*Administrator*“ auf der Schulkonsole des Servers („*server.paedml-linux.lokal*“) oder auf der Schulkonsole des *opsi*-Servers („*backup.paedml-linux.lokal*“) an. Wählen Sie im Menü „*System*“ den Untermenüpunkt „*Neustarten*“ aus und im nächsten Fenster die Aktion „*Herunterfahren*“.
3. **Über Textkonsole:** Anmelden als Benutzer „*root*“ auf der Konsole der VM „*Server*“ bzw. „*opsi-Server*“, dann `#shutdown -h now`“ ausführen.

Vom „harten Ausschalten“ aus dem *vSphere-Client* heraus über „*Betrieb* | *Ausschalten*“ sollte unbedingt abgesehen werden!

Erstellen des Snapshots der VM „Server“
Rechtsklick auf die virtuelle Maschine „*Server*“, Auswahl von „*Snapshot* | *Snapshot erstellen…*“

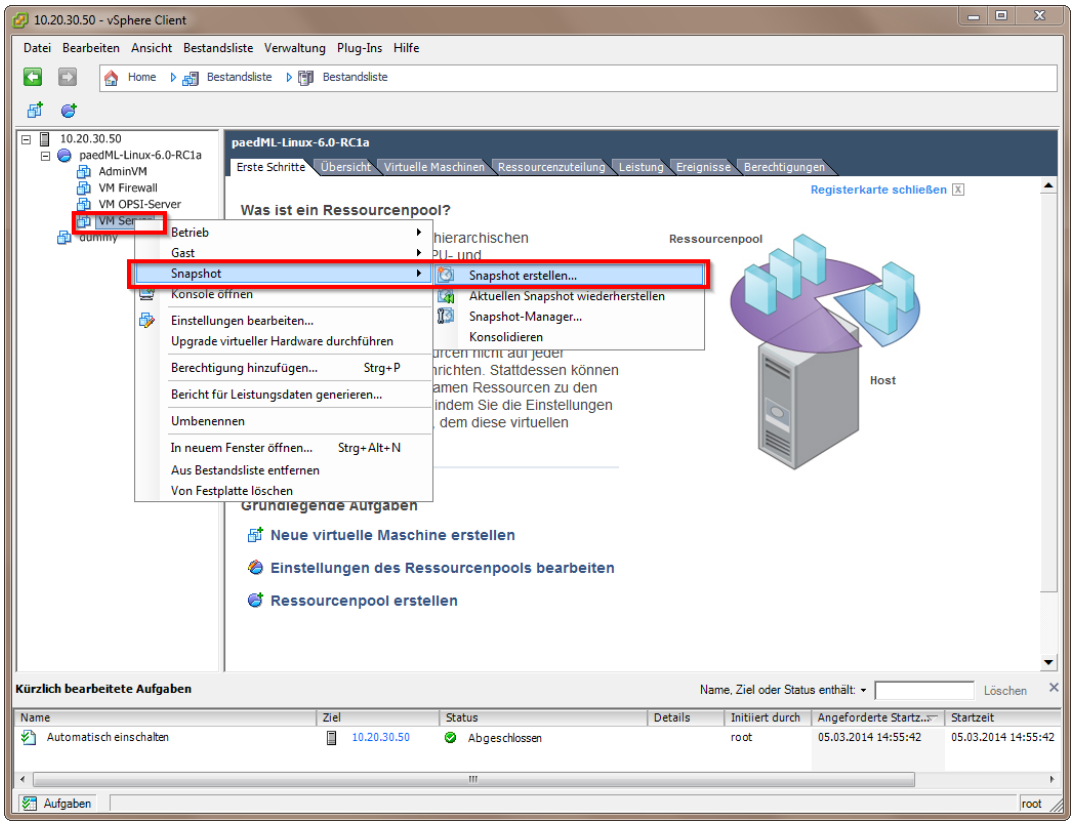


Abb. 226: Erstellen eines Snapshots der VM „Server“

Vergeben Sie einen aussagekräftigen Namen für den Snapshot sowie eine ausführliche Beschreibung und starten Sie den Vorgang mit „*OK*“. Der Snapshot wird anschließend erstellt.

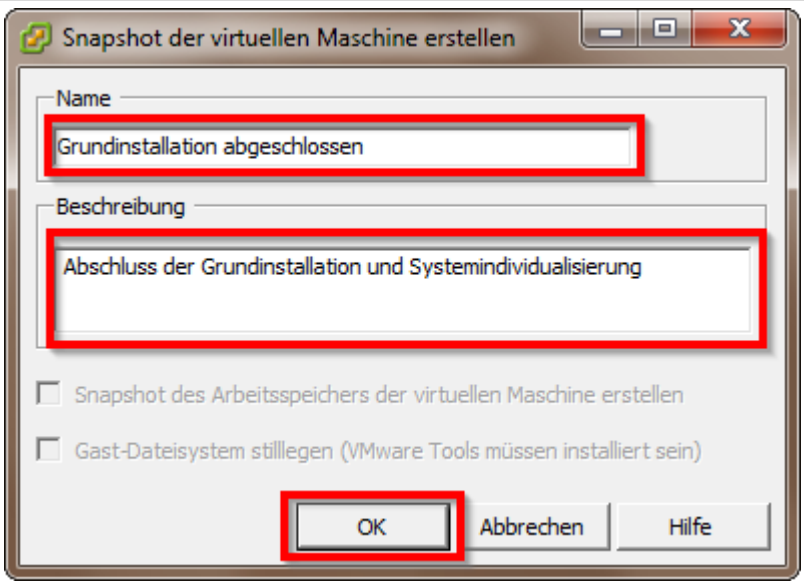


Abb. 227: Name und Beschreibung des Snapshots angeben.

Erstellen des Snapshots der VM „*opsi-Server*“

Erstellen Sie auf gleiche Art und Weise einen Snapshot der VM „*opsi-Server*“. Vergeben Sie dabei ebenfalls einen aussagekräftigen Namen und eine ausführliche Beschreibung. Empfohlen wird außerdem die Namen der Snapshots anzupassen, um bei der Wiederherstellung den gleichen Versionsstand der zusammengehörenden Snapshots wieder herzustellen. Dies kann beispielsweise über einen Timestamp im Namen des Snapshots geschehen.

Beispiele für Namen von Snapshots:

- Server-2014-07-09
- Backup-Server-2014-07-09

Der Fortschritt der Snapshots kann im unteren Bereich des *vSphere-Clients* beobachtet werden.

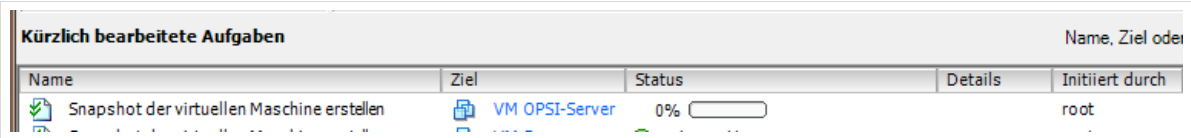


Abb. 228: Snapshot einer virtuellen Maschine wird erstellt.

Wenn beide Snapshots angelegt sind, wird dies wie folgt im *vSphere-Client* angezeigt:

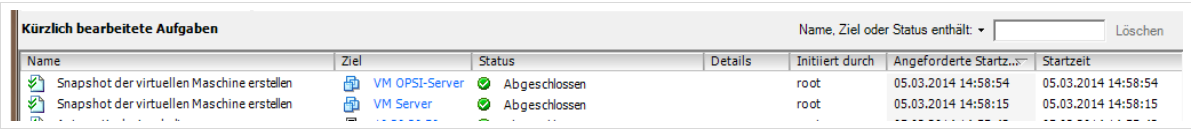


Abb. 229: Anlegen der Snapshots ist abgeschlossen

Hochfahren der virtuellen Maschinen

Fahren Sie abschließend die beiden virtuellen Maschinen wieder hoch.

10.3Wiederherstellen eines Snapshots

Beim Wiederherstellen eines Snapshots werden die virtuellen Maschinen „*server*“ und „*backup*“ vollständig auf den Stand des Erstellungszeitpunkts des Snapshots zurückgesetzt. Die beiden Maschinen können nur zusammen wiederhergestellt werden. Dies setzt voraus, dass von beiden Maschinen Snapshots zum gleichen Zeitpunkt angefertigt wurden.

Achtung, potentieller Datenverlust!

Beim Wiederherstellen eines Snapshots werden sämtliche System-Einstellungen und Benutzerdaten auf den Stand des Snapshots zurückgesetzt.

Nach Erstellung des Snapshots geänderte Daten (neu angelegte/geänderte Dateien von Benutzern, geänderte Benutzerkonten, Konfigurationsänderungen am System, Änderungen von Benutzerpasswörtern,…) gehen verloren.

Herunterfahren der beiden virtuellen Maschinen

Fahren Sie die beiden virtuellen Maschinen „*server*“ und „*backup*“ herunter.

Optional: Anlegen eines Snapshots

Da der aktuelle Zustand der virtuellen Maschinen beim Wiederherstellen eines anderen Snapshots unwiederbringlich verloren geht, sollte an dieser Stelle überlegt werden, ob das Anlegen eines neuen Snapshots vor der Wiederherstellung eines alten Snapshots sinnvoll ist.

Wiederherstellen eines Snapshots der VM „Server“

Klicken Sie im *vSphere-Client* mit Rechts auf die VM „*server*“ und wählen Sie „*Snapshot | Snapshot-Manager…“:*

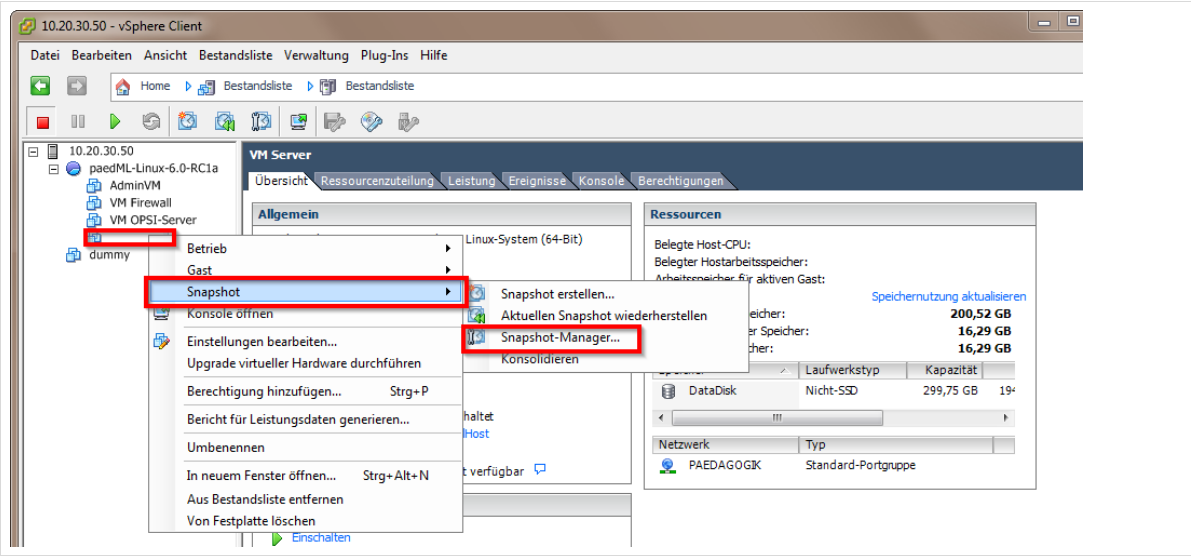


Abb. 230: Öffnen des Snapshot-Managers

Wählen Sie nun denjenigen Snapshot aus, auf den Sie zurückwechseln möchten und klicken Sie auf „*Wechseln zu*“:

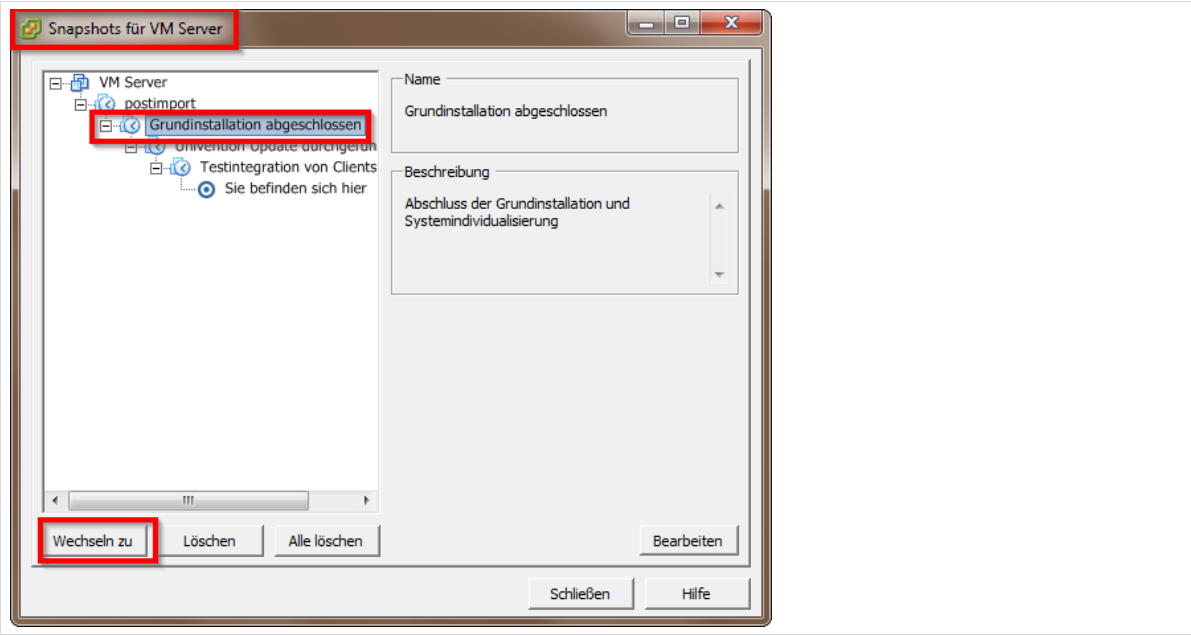


Abb. 231: Auswahl eines angelegten Snapshots

Bestätigen Sie die Sicherheitsabfrage, um die Wiederherstellung des Snapshots anzustoßen

Bestätigen
Der aktuelle Zustand der virtuellen Maschine geht verloren, wenn er nicht in einem Snapshot gespeichert wurde. Möchten Sie Snapshot 'Grundinstallation abgeschlossen' wiederherstellen?
Ja
Nein

Abb. 232: Sicherheitsabfrage vor dem Endgültigen Wechsel zu einem früheren Snapshot

Schließen Sie das Fenster des Snapshot-Managers über den Knopf „*Schließen*“

Wiederherstellen des passenden Snapshots der VM „*opsi-Server*“
Stellen Sie anschließend den Snapshot der VM „*opsi-Server*“ wieder her. Achten Sie darauf, dass sie den zur VM „*Server*“ passenden Snapshot auswählen:

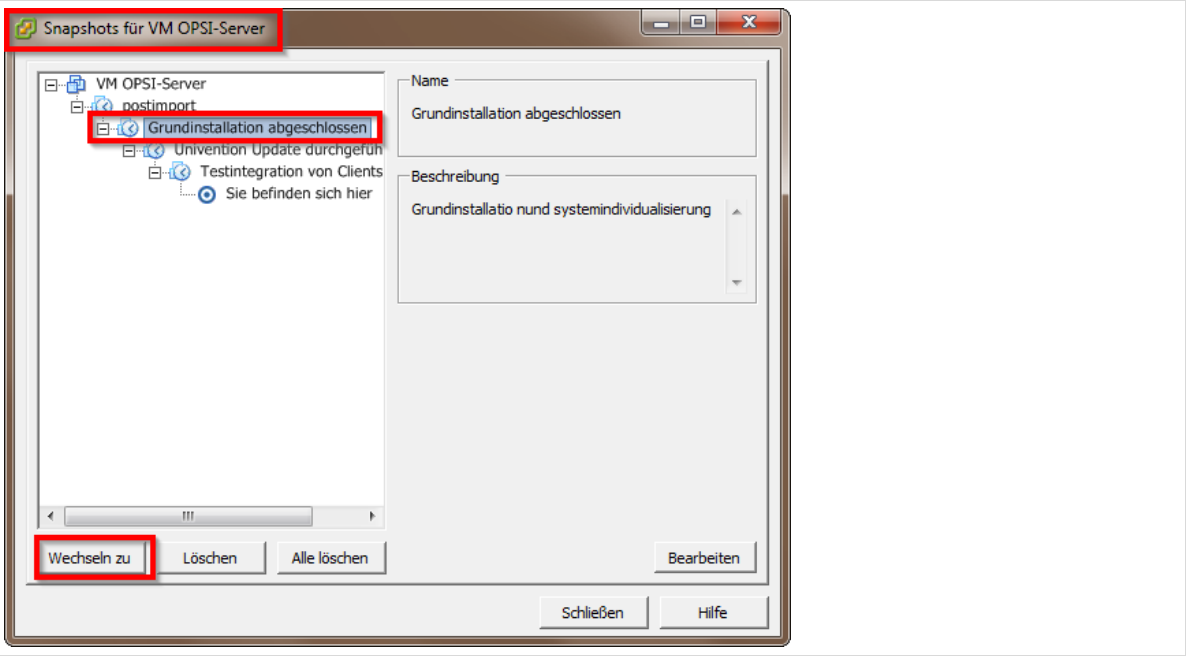


*Abb. 233: Auswahl des richtigen Snapshots für die VM „*opsi-Server*“*

Hochfahren der virtuellen Maschinen
Fahren Sie anschließend beide Maschinen wieder hoch.

Optional: Domänenmitgliedschaft der Clients wiederherstellen
Beim Wiederherstellen der virtuellen Maschinen kann es vorkommen, dass Clients ihre Domänenzugehörigkeit verlieren, da die *Windows*-Clients in regelmäßigen Abständen die Kennwörter ihrer Domänenkonten ändern.

Ein Snapshot, der die letzte Kennwortänderung der *Windows*-Clients nicht enthält, führt dazu, dass sich Benutzer, bzw. Rechner nicht mehr an der Domäne anmelden können.

Falls ein erneuter Domänenbeitritt der Clients notwendig sein sollte, kann dieser über das *opsi*-Produkt *windomain* angestoßen werden. Um den Rechner wieder in die Domäne aufzunehmen, muss das Paket *windomain* erneut auf dem Rechner installiert werden. Genauere Informationen zu *opsi* finden Sie im Administrationshandbuch.

Dieses Verfahren gilt nur, wenn der Rechner wieder in die gleiche Domäne aufgenommen werden soll, deren Mitglied er schon war.

Wenn der Rechner einer neuen Domäne, zum Beispiel nach Server-Neuinstallation, hinzugefügt werden soll, funktioniert das Verfahren nicht.

10.4 Verwalten von Snapshots

Snapshots stellen vor allem bei Konfigurationsänderungen am *paedML Linux* System, eine bequeme Art dar, jederzeit wieder auf einen funktionierenden Zustand zurückwechseln zu können. Hierüber können gefahrlos Konfigurationsänderungen getestet werden. Es sollten jedoch nicht bedenkenlos zu viele Snapshots angelegt werden, denn

- das Bevorraten mehrerer Snapshots kann unter Umständen massiv Festplattenplatz belegen, da im Snapshot alle Benutzerdaten gespeichert sind.
- bei Snapshots werden – vereinfacht dargestellt – nur die Unterschiede zu Vorgänger-Snapshots gespeichert. Beim Betrieb mit mehreren Snapshots besteht der aktuelle „Zustand“ aus einem Grundzustand und mehreren Änderungen. Der häufige Gebrauch von Snapshots kann sich negativ auf die Performance des Systems auswirken.

Löschen von Snapshots

Um Speicherplatz zu sparen, können „alte“, nicht mehr benötigte Snapshots gelöscht werden. Das Löschen von „alten“ Snapshots ist jedoch eine sehr aufwändige Operation, da die Daten des gelöschten Snapshots unter Umständen in einen darauf basierenden späteren Snapshot integriert werden müssen. Darum sollte das Löschen von Snapshots ebenfalls nur bei ausgeschalteter VM durchgeführt werden.

Löschen Sie Snapshots einer virtuellen Maschine nur dann, wenn diese ausgeschaltet ist!

10.5 Snapshots der Firewall

Die Firewall speichert jede Konfigurationsänderung in einer separaten XML-Konfigurationsdatei im Ordner */conf/backup*. Diese Änderungen können jederzeit über die grafische Oberfläche wiederhergestellt werden. Daher ist eine Sicherung der Firewall über Snapshots eigentlich nicht notwendig.

Einzig bei der Individualisierung des *paedML Linux*-Systems mittels `lmz-initial-setup`, die einmalig bei der Erstinstallation durchgeführt wird, werden Änderungen an der Firewall durchgeführt (Änderung von root-passwort, SSH-Key, und SSL-Zertifikat), die das Anlegen eines Snapshots technisch begründen.

Um administrative Arbeitsabläufe zu vereinheitlichen, **kann** die VM *Firewall* jedoch genau wie oben beschrieben mittels Snapshots gesichert werden. Eine zeitlich gemeinsame Sicherung bzw. Wiederherstellung mit den Maschinen „*Server*“ bzw. „*backup*“ kann erfolgen, ist jedoch nicht notwendig.

10.6 Snapshots weiterer virtueller Maschinen

Für eventuell weitere im System befindliche Maschinen (z.B. „*adminvm*“) können natürlich ebenfalls Snapshots angelegt werden. Diese können auch zeitlich unabhängig von den Maschinen „*server*“ und „*backup*“ angelegt und wiederhergestellt werden.

Es wird empfohlen einen Snapshot der *Admin-VM* zu erstellen, sobald die Aktivierung der *Windows*-Rechner im Schulnetz durchgeführt wurde.

Nach (Neu-)Aufnahme von *Windows*-Rechnern und deren Aktivierung ergibt es ebenfalls Sinn einen Snapshot der Admin-VM zu erstellen

11. Erweiterungsmöglichkeiten der *paedML Linux*

Die *paedML Linux* bietet Erweiterungsmöglichkeiten, die im Folgenden beschrieben werden.

11.1 Integration weiterer Server

Die *paedML Linux* kann durch den Betrieb weiterer Server auf individuelle Bedürfnisse angepasst bzw. erweitert werden. Für den Betrieb dieser Server ist ein spezieller IP-Bereich vorgesehen, um (zukünftige) Konflikte mit dem *paedML Linux* System zu vermieden.

Auf den bestehenden Servern dürfen keine weiteren Services (z.B. Webserver, Datenbankserver) installiert werden..

Sollen innerhalb des Schulnetzes weitere Services (z.B. Webserver, Datenbankserver für Unterrichtszwecke) betrieben werden, so darf dies nicht auf den virtuellen *paedML* Servern geschehen[5]. Für diese Zwecke müssen eine oder mehrere weitere virtuelle Maschinen auf dem Virtualisierungs-Host angelegt werden und ins Netz „*PAEDAGOGIK*“ eingebunden werden.

Für die Installation eines eigenen virtuellen Servers gibt es mehrere Möglichkeiten:

- Virtualisierung einer bereits bestehenden physikalischen Maschine.
- Neuinstallation von CD bzw. ISO-Datei.
- Verwenden von vorkonfigurierten VMware-Images (als ..zip-Archiv oder OVF-Vorlage), die direkt auf den Hypervisor importiert werden können. Dazu gibt es im Internet ein reichhaltiges Angebot für die unterschiedlichsten Einsatzwecke, zum Beispiel unter
  - Turnkey Linux (http://www.turnkeylinux.org)
  - Bitnami (http://www.bitnami.com)

Netzanbindung

Im Netz „*PAEDAGOGIK*“ ist der IP-Adressbereich *10.1.0.1 – 10.1.0.31* reserviert, Adressen oberhalb von *10.1.0.31* werden vom DHCP-Server für die Client-Rechner vergeben.

Der Bereich *10.1.0.1 – 10.1.0.20* ist für *paedML Linux*-eigene Maschinen reserviert (z.B. Server, Firewall oder Router zur Anbindung weiterer Netze). Diese IP-Adressen dürfen nicht für eigene Server verwendet werden!

Der Bereich *10.1.0.21 – 10.1.0.31* kann für zusätzliche Server genutzt werden. Wählen Sie eine IP aus diesem Bereich aus.

[5] Leider zeigt die Erfahrung, dass Modifikationen an Systemdiensten häufig zu Fehlern im Betrieb der *paedML* führen. Um dies zu vermeiden, sollten eigenständige Anpassungen an den *paedML* Maschinen weitestgehend vermieden werden.

IP-Bereich	Verwendung
10.1.0.1 – 10.1.0.20	reservierte IP-Adressen für *paedML Linux* VMs
10.1.0.21 – 10.1.0.31	IPs-Adressen für weitere Server

Tabelle 6: Aufteilung des unteren IP-Bereichs

Auch wenn zum jetzigen Zeitpunkt nicht alle IP-Adressen aus dem Bereich *10.1.0.1* bis *10.1.0.20* in Verwendung sind, kann dies in späteren *paedML Linux*-Versionen durchaus der Fall sein. Verwenden Sie keine IP-Adressen aus diesem Bereich für eigene Maschinen!

Abhängig vom Einsatzzweck der zusätzlichen Server müssen eventuell noch weitere Konfigurationen durchgeführt werden.

11.2 Vergrößern der Festplatten der VM „Server“

Falls die im Auslieferungszustand definierten Festplattengrößen der virtuellen Server nicht ausreichen, können diese vergrößert werden.

Wenn die Rede von „Festplatten“ ist, muss zwischen den folgenden Begriffen unterschieden werden.

- **Physische Festplatten des Virtualisierungs-Hosts**: Reale Festplatten, die entweder intern (SCSI, SATA) im Virtualisierungs-Host eingebaut oder z.B. per SAN mit dem Hypervisor verbunden sind.
- **Datastores**: Im Hypervisor eingerichtete Partitionen auf den physikalischen Festplatten, auf denen virtuelle Maschinen einschließlich ihrer virtuellen Festplattenabbilder gespeichert werden.
- **virtuelles Festplattenabbild**: Eine oder mehrere zusammengehörige Dateien (z.B. „*my-vm-disk001.vmdk*“), innerhalb eines Datastores des Hypervisors, innerhalb der die Daten für eine Festplatte einer virtuellen Maschine gespeichert werden. **Festplatte einer virtuellen Maschine**: Jede VM benötigt in der Regel mindestens eine Festplatte. Diese wird beim Anlegen (oder beim Import) der VM erstellt und besitzt eine festgelegte Größe (z.B. 60 GB).

Soll die Festplatte einer virtuellen Maschine vergrößert werden, dann sind grundsätzlich zwei verschiedene Verfahren denkbar:

- Hinzufügen einer weiteren Festplatte: Es wird eine weitere Festplatte in die virtuelle Maschine „eingebaut“.
- Vergrößern der virtuellen Festplatte: Eine bestehende Festplatte der VM wird nachträglich vergrößert, dabei bleibt zunächst die alte Partitionstabelle erhalten.

11.2.1 Hinzufügen einer Festplatte zu einer virtuellen Maschine

Das Verändern der Festplattenkonfiguration stellt einen massiven Eingriff in die Konfiguration des gesamten paedML-Systems dar. Im Fehlerfall kann ein vollständiger Datenverlust eintreten.

Sichern Sie vor der Anpassung der Festplattenkonfiguration alle virtuellen

Festplattenabbilder auf einem externen Speichermedium.

Stellen Sie zunächst sicher, dass auf dem Datastore des Virtualisierungs-Hosts genügend Speicherplatz für die neue Festplatte vorhanden ist.

Loggen Sie sich im *vSphere-Client* ein und wählen Sie die VM aus, zu der Sie eine weitere Festplatte hinzufügen möchten. Klicken Sie im Reiter „*Übersicht*“ auf „*Einstellungen bearbeiten*“.

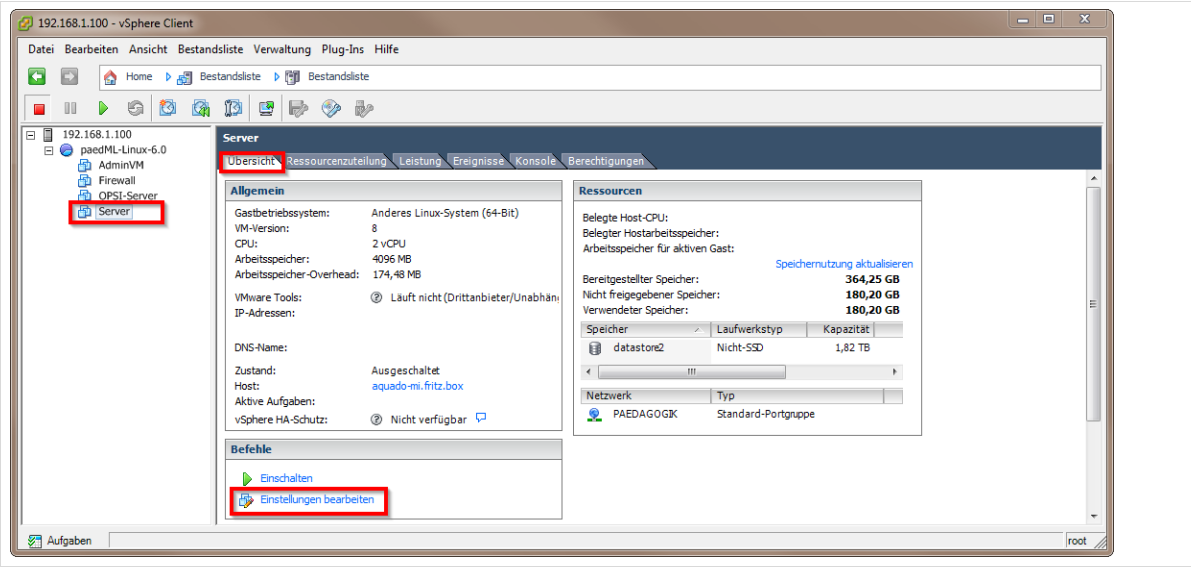


Abb. 234: Bearbeiten der Einstellungen der VM

Klicken Sie im nächsten Fenster auf „*Hinzufügen*“, um ein neues Gerät anzulegen.

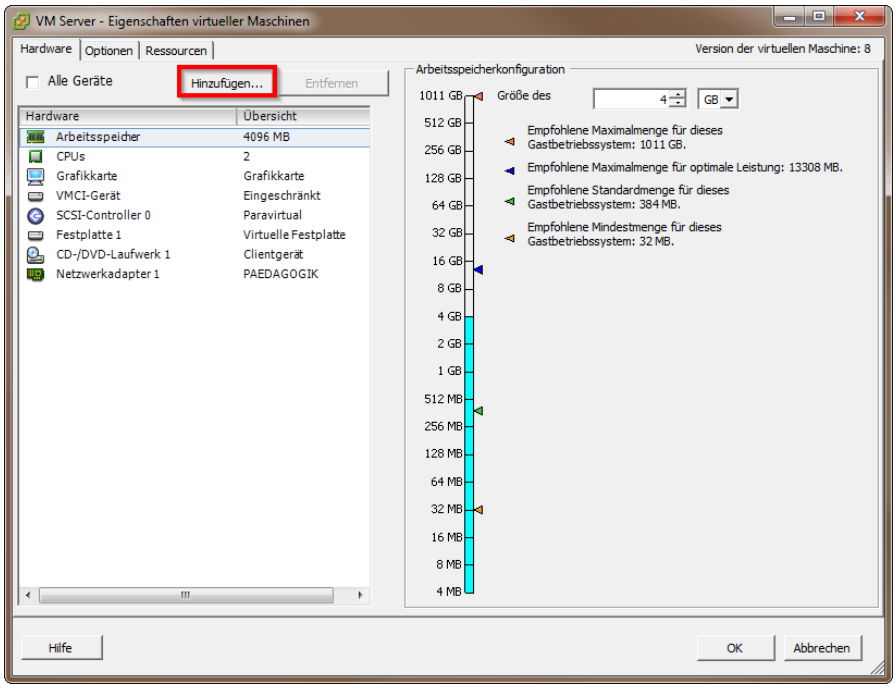


Abb. 235: Hinzufügen eines neuen Geräts zu einer virtuellen Maschine

Wählen Sie den Gerätetyp „*Festplatte*“ aus und klicken Sie auf „*Weiter*“.

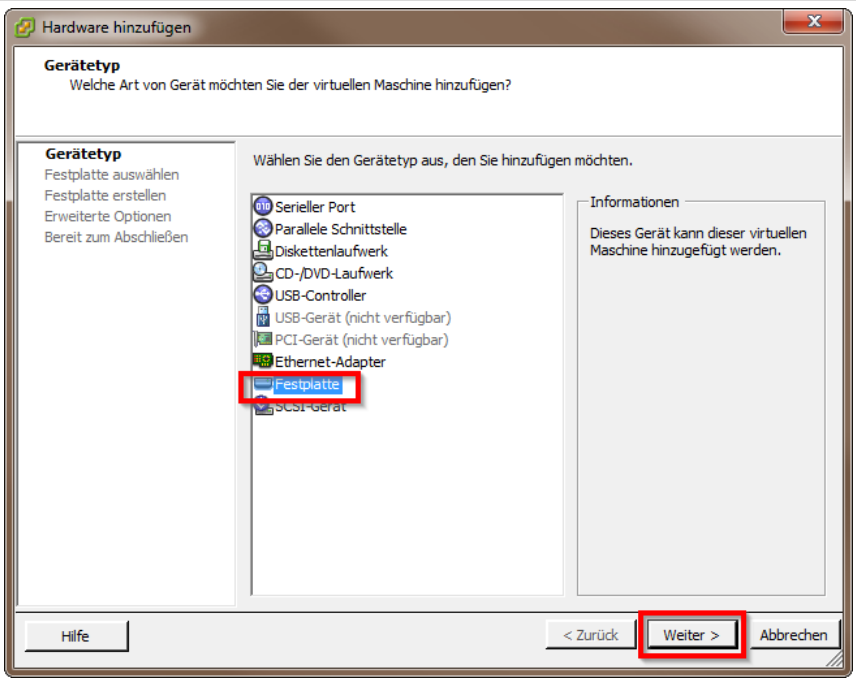


Abb. 236: Auswahl des Gerätetyps „Festplatte“

Wählen Sie als Festplattentyp „*Neue virtuelle Festplatte erstellen*“ aus und klicken Sie auf „*Weiter*“.

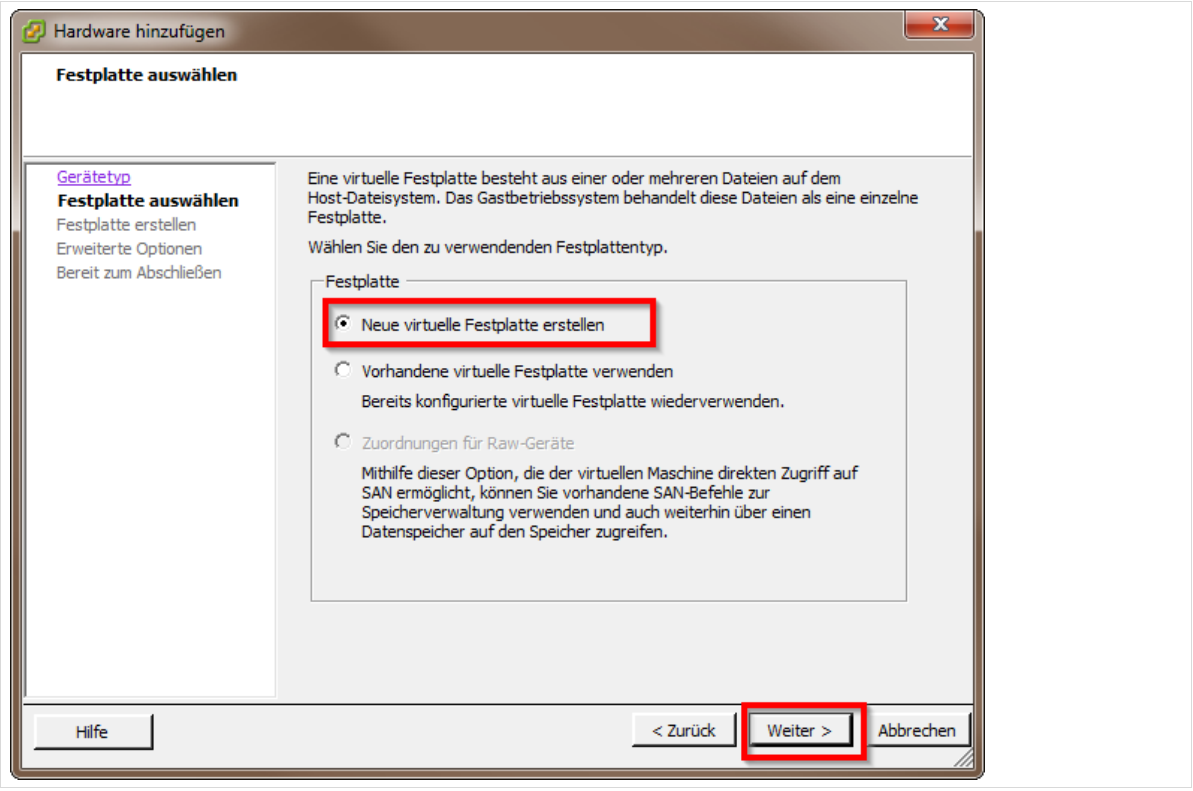

Hardware hinzufügen
Festplatte auswählen
Gerätetyp
Festplatte auswählen
Festplatte erstellen
Erweiterte Optionen
Bereit zum Abschließen
Eine virtuelle Festplatte besteht aus einer oder mehreren Dateien auf dem Host-Dateisystem. Das Gastbetriebssystem behandelt diese Dateien als eine einzelne Festplatte.
Wählen Sie den zu verwendenden Festplattentyp.
Festplatte
Neue virtuelle Festplatte erstellen
Vorhandene virtuelle Festplatte verwenden
Bereits konfigurierte virtuelle Festplatte wiederverwenden.
Zuordnungen für Raw-Geräte
Mithilfe dieser Option, die der virtuellen Maschine direkten Zugriff auf SAN ermöglicht, können Sie vorhandene SAN-Befehle zur Speicherverwaltung verwenden und auch weiterhin über einen Datenspeicher auf den Speicher zugreifen.
Hilfe
< Zurück
Weiter >
Abbrechen

Abb. 237: Festplattentyp „Neue virtuelle Festplatte“

Legen Sie im nächsten Fenster die gewünschte *Festplattengröße* ,die Provisionierungs-Art „*Thick Provision Eager-Zeroed*“ und den *Speicherort* fest und klicken Sie auf „*Weiter*“.

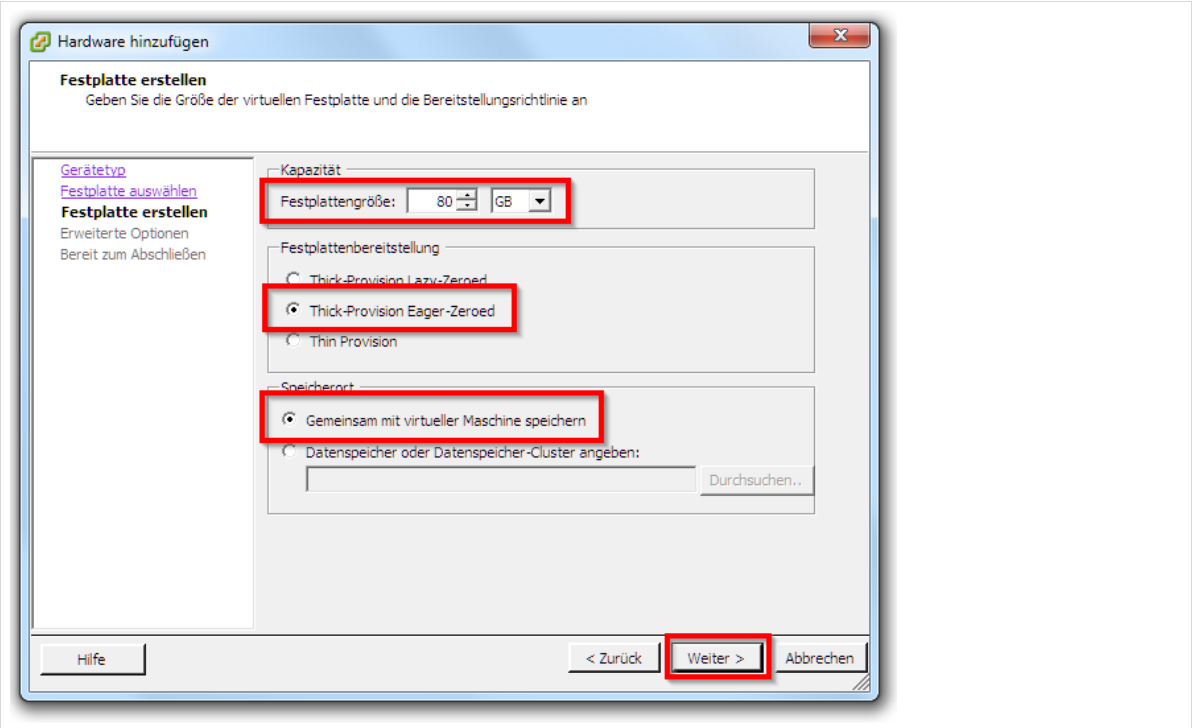


Abb. 238: Festlegen von Festplattengröße und Provisionierungs-Art.

Wählen Sie im nächsten Fenster die Standardeinstellung „*SCSI*“ aus. Der Haken bei „*Unabhängig*“ darf nicht gesetzt sein.

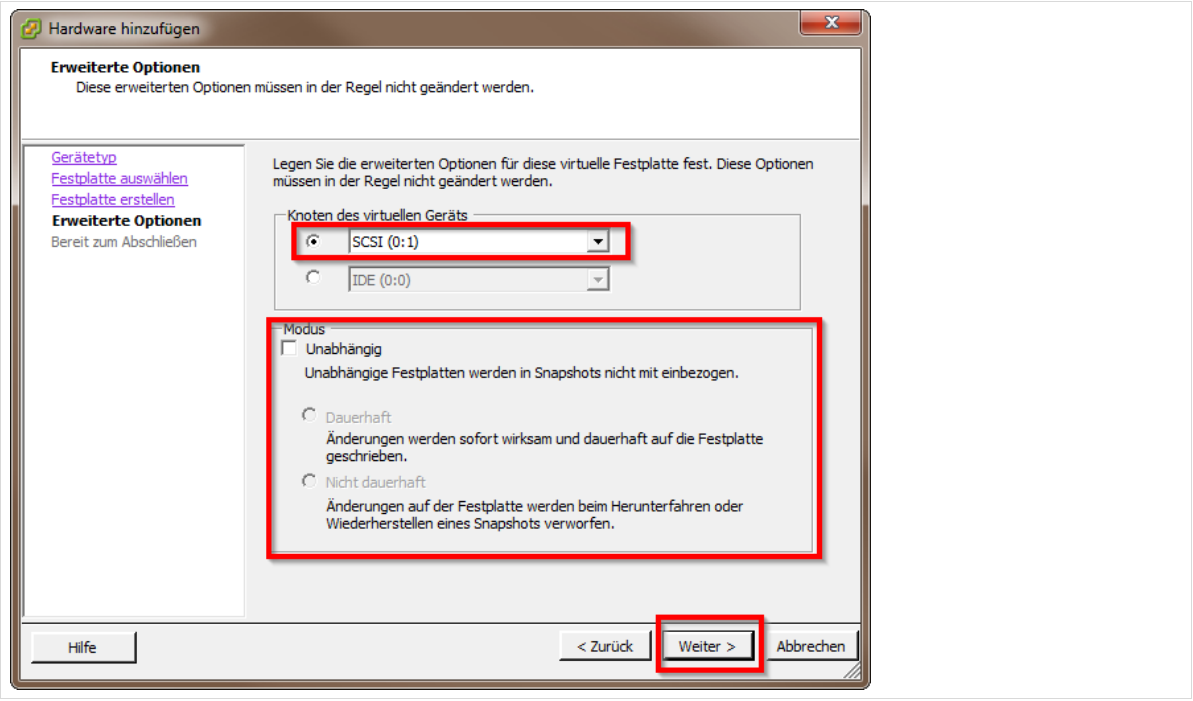

Hardware hinzufügen
Erweiterte Optionen
Diese erweiterten Optionen müssen in der Regel nicht geändert werden.
Gerätetyp
Festplatte auswählen
Festplatte erstellen
Erweiterte Optionen
Bereit zum Abschließen
Legen Sie die erweiterten Optionen für diese virtuelle Festplatte fest. Diese Optionen müssen in der Regel nicht geändert werden.
Knoten des virtuellen Geräts
SCSI (0:1)
IDE (0:0)
Modus
Unabhängig
Unabhängige Festplatten werden in Snapshots nicht mit einbezogen.
Dauerhaft
Änderungen werden sofort wirksam und dauerhaft auf die Festplatte geschrieben.
Nicht dauerhaft
Änderungen auf der Festplatte werden beim Herunterfahren oder Wiederherstellen eines Snapshots verworfen.
Hilfe
< Zurück
Weiter >
Abbrechen

Abb. 239: Erweiterte Optionen der neuen Festplatte

Überprüfen Sie im nächsten Fenster nochmals alle Angaben, bevor Sie die neue Festplatte durch Klick auf „*Beenden*“ anlegen.

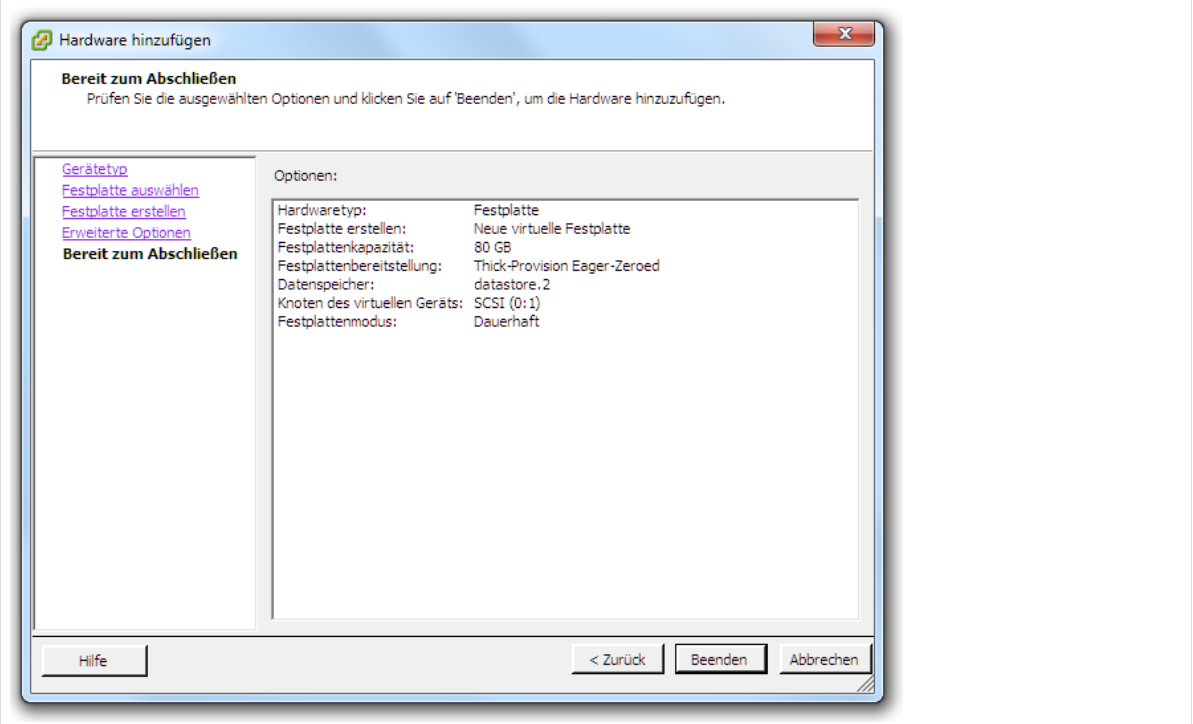


Abb. 240: Überprüfen aller Optionen

Daraufhin wird eine neue Festplatte angelegt. Klicken Sie auf „*OK*“ um wieder zur Übersichtsseite des *vSphere-Client* zu gelangen.

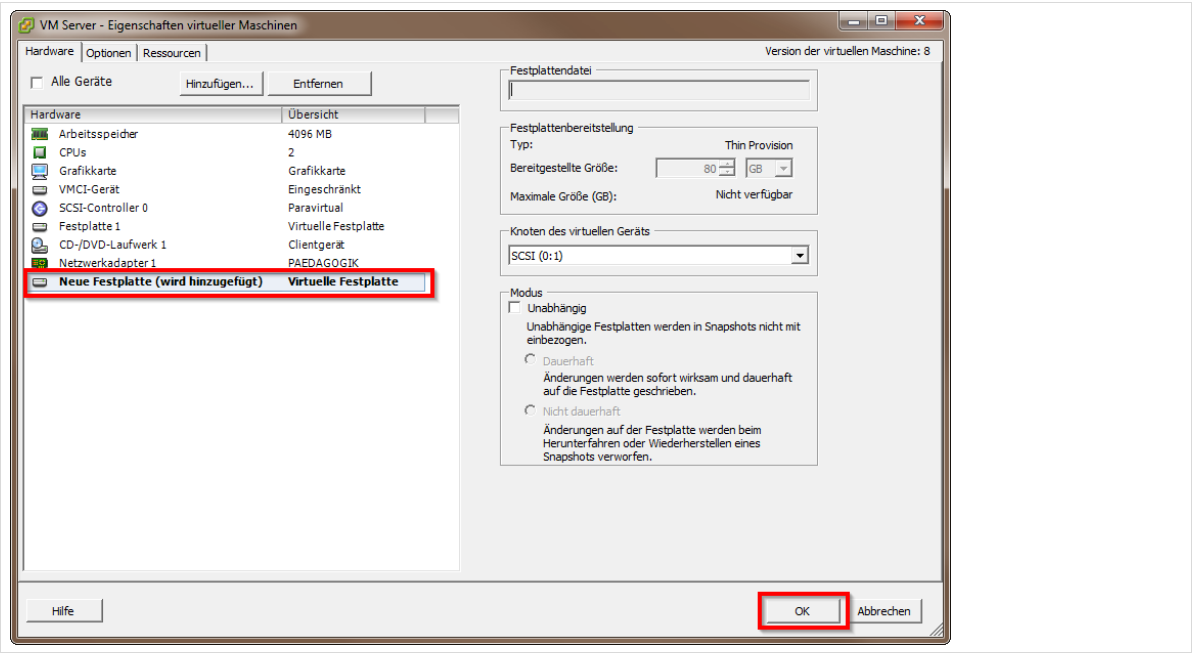


Abb. 241: Die neue Festplatte wird angelegt.

Nachdem die neue Festplatte angelegt wurde, sollte diese in den Einstellungen der virtuellen Maschine wie folgt erscheinen:

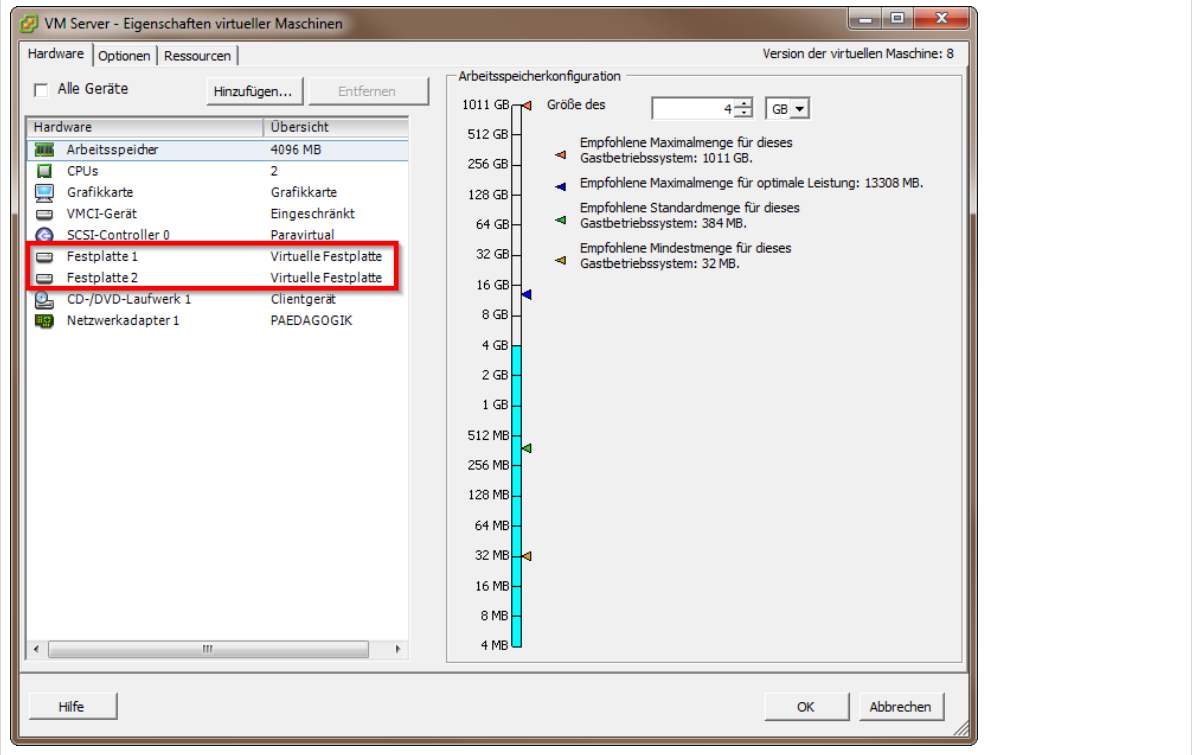


Abb. 242: Die neue Festplatte wurde erfolgreich angelegt.

11.2.2 Vorbereiten der neuen Festplatte

Achten Sie im Folgenden darauf, was Sie eintippen. Ein falsches Zeichen kann die gesamte *paedML Linux*-Installation unbrauchbar machen! Im Folgenden wird die Änderung der Datenträger mit dem Linux-Werkzeug *fdisk* beschrieben. Bei Änderungen gehen alle auf der Festplatte vorhandenen Daten verloren. Erstellen Sie bei Bedarf vorher eine Datensicherung.

Loggen Sie sich als nächstes auf der Konsole der virtuellen Maschine als *root* ein.

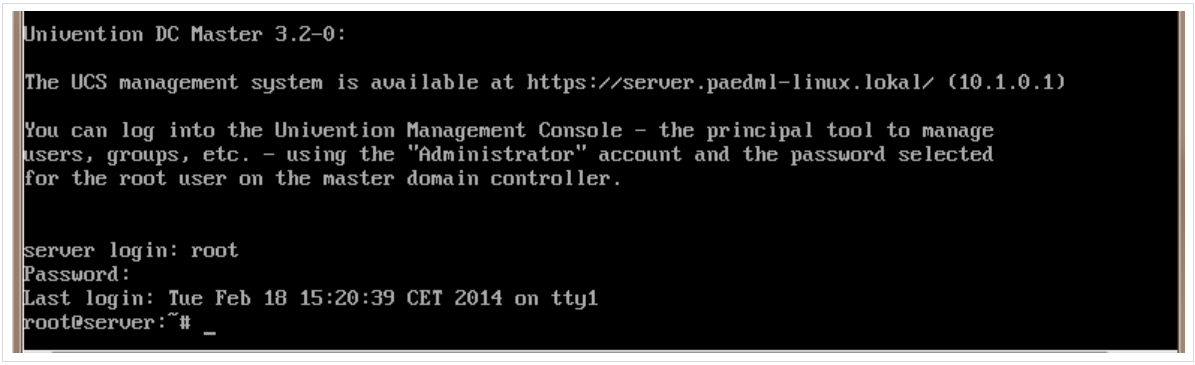

Univention DC Master 3.2-0:
The UCS management system is available at https://server.paedml-linux.lokal/ (10.1.0.1)
You can log into the Univention Management Console - the principal tool to manage
users, groups, etc. - using the "Administrator" account and the password selected
for the root user on the master domain controller.
server login: root
Password:
Last login: Tue Feb 18 15:20:39 CET 2014 on tty1
root@server:~# _

Abb. 243: Login auf der Konsole des Servers

11.2.2.1 Anlegen einer neuen Partitionstabelle

Mit dem Befehl `#fdisk -l` können sich eine Liste der am System angeschlossenen Geräte ausgeben lassen.

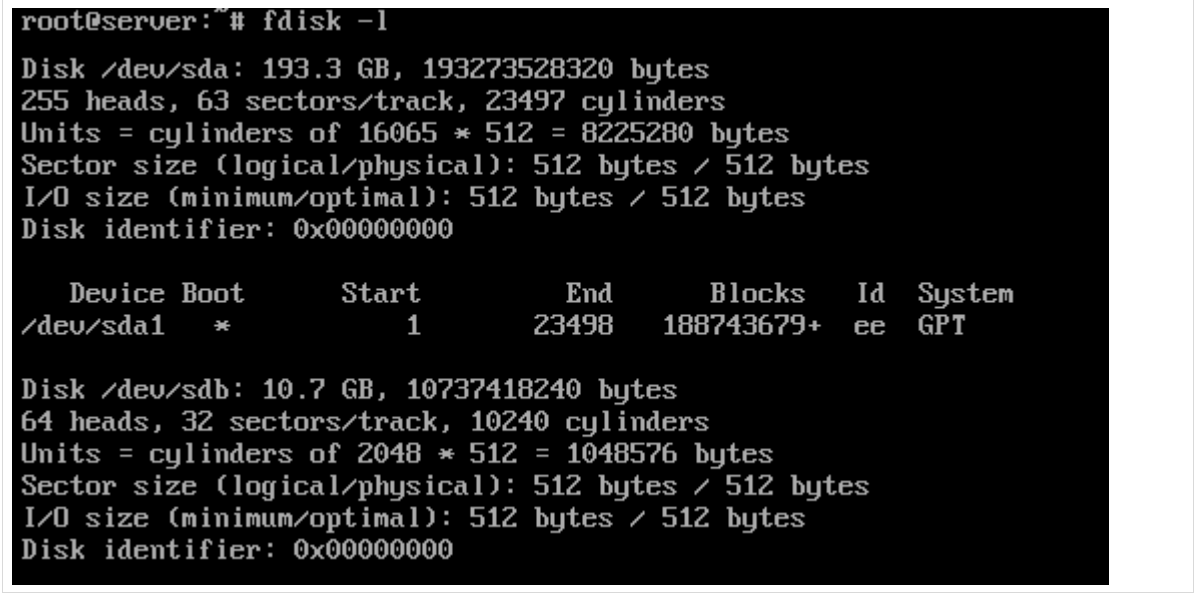

root@server:~# fdisk -l
Disk /dev/sda: 193.3 GB, 193273528320 bytes
255 heads, 63 sectors/track, 23497 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000
Device Boot Start End Blocks Id System
/dev/sda1 * 1 23498 188743679+ ee GPT
Disk /dev/sdb: 10.7 GB, 10737418240 bytes
64 heads, 32 sectors/track, 10240 cylinders
Units = cylinders of 2048 * 512 = 1048576 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

Abb. 244: Ausgabe der am System angeschlossenen Festplatten via fdisk

Zunächst muss auf der neu angelegten Festplatte eine Partitionstabelle angelegt werden, starten Sie dazu das Partitionierungstool *fdisk* unter Angabe der Gerätedatei der neu angelegten Platte. Normalerweise wird dies */dev/sdb* sein.

Beispiel:

```
#fdisk /dev/sdb
```

Eine Liste aller in *fdisk* verfügbaren Befehle erhalten Sie durch Drücken der Tasten h oder m.

- Drücken Sie die Taste o, um eine neue, leere Partitionstabelle anzulegen.
- Drücken Sie danach die Taste w, um die Änderungen tatsächlich durchzuführen.
- Drücken Sie q, falls Sie fdisk verlassen wollen ohne Änderungen zu speichern.

11.2.2.2 Anlegen einer Partition

Starten Sie das Tool *fdisk* erneut unter Angabe der Gerätedatei der neuen Festplatte:

Beispiel:

```
#fdisk /dev/sdb
```

- Drücken Sie die Taste n, um eine neue Partition anzulegen
- Drücken Sie p für „primäre Partition“.
- Drücken Sie 1, um die Nummer der anzulegenden Partition anzugeben.
- Übernehmen Sie die Voreinstellung für „*first cylinder*“ durch Drücken von Enter
- Übernehmen Sie die Voreinstellung für „*last cylinder*“ durch Drücken von Enter.
- Drücken Sie w um die Änderungen tatsächlich durchzuführen.

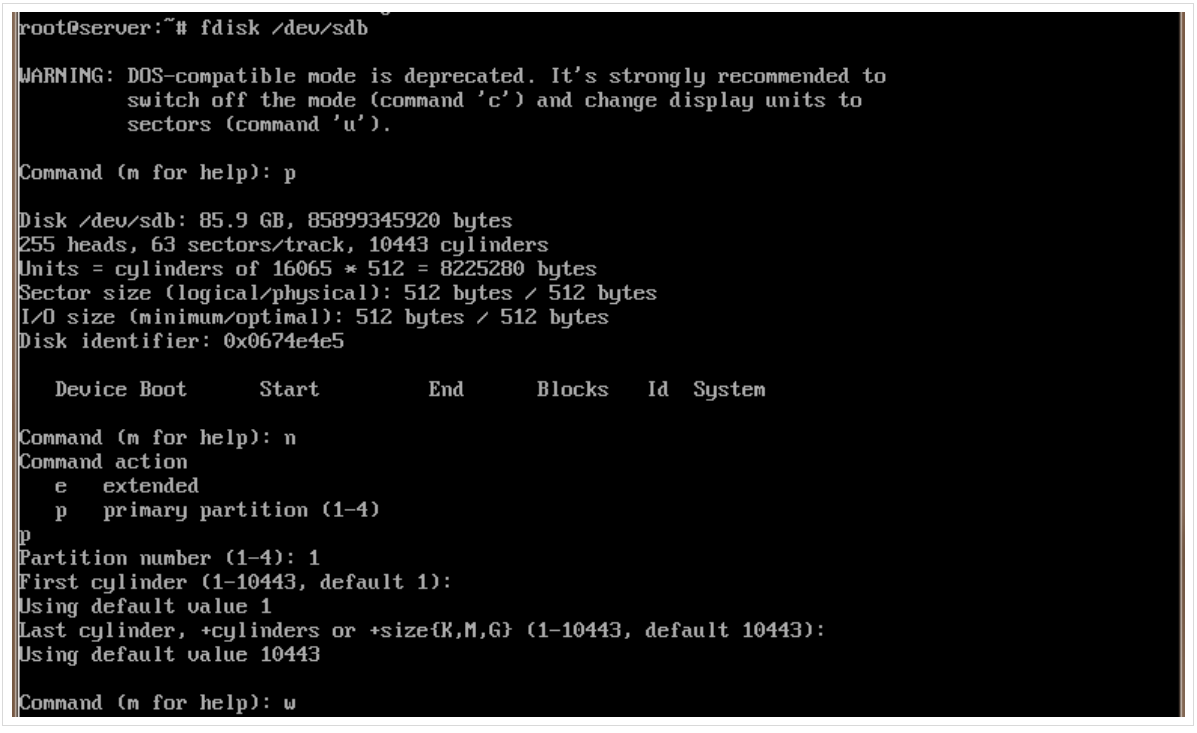

root@server:~# fdisk /dev/sdb
WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
switch off the mode (command 'c') and change display units to
sectors (command 'u').
Command (m for help): p
Disk /dev/sdb: 85.9 GB, 85899345920 bytes
255 heads, 63 sectors/track, 10443 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x0674e4e5
Device Boot Start End Blocks Id System
Command (m for help): n
Command action
e extended
p primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-10443, default 1):
Using default value 1
Last cylinder, +cylinders or +size{K,M,G} (1-10443, default 10443):
Using default value 10443
Command (m for help): w

Abb. 245: Anlegen einer neuen Partition

Überprüfen Sie anschließend die Partitionierung durch Eingabe von `fdisk -l <Gerätedatei>`

Beispiel:

```
#fdisk -l /dev/sdb
```

In der Ausgabe sollte die neue Partitionstabelle mit einer einzigen Partition erscheinen:

```
root@server:~# fdisk -l /dev/sdb

Disk /dev/sdb: 85.9 GB, 85899345920 bytes
255 heads, 63 sectors/track, 10443 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x0674e4e5

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1               1       10443    83883366   83  Linux
root@server:~# _
```

Abb. 246: Überprüfen der neu angelegten Partition

11.2.2.3 Formatieren der Partition als „Physical Volume“

Im nächsten Schritt muss die Partition mit dem Tool „*pvcreate*“ als sogenannte „*Physical Partition*“ formatiert werden, um vom *Logical Volume Manager* (*LVM*) genutzt werden zu können.

Beispiel:

```
# pvcreate /dev/sdb1
```

11.2.2.4 Erweitern der Volume Group „vg_ucs“

Die neue Partition muss nun in die Volume Group „*vg_ucs*“ des LVM aufgenommen werden, damit der Speicherplatz genutzt werden kann:

Beispiel:

```
# vgextend vg_ucs /dev/sdb1
```

Überprüfen Sie, ob die Partition korrekt in die volume group „*vg_ucs*“ aufgenommen wurde mit

```
# lvm pvscan
```

In der Ausgabe sollte die neu hinzugefügte Platte als Bestandteil des Volume Group „*vg_ucs“* angezeigt werden.:

root@server:~# lvm pvscan
PV /dev/sda4 VG vg_ucs lvm2 [175,85 GiB / 16,00 MiB free]
PV /dev/sdb1 VG vg_ucs lvm2 [80,00 GiB / 80,00 GiB free]
Total: 2 [255,84 GiB] / in use: 2 [255,84 GiB] / in no VG: 0 [0]
root@server:~# _

Abb. 247: Die neue Partition wurde in die Volume Group „vg_ucs“ aufgenommen.

Damit steht der Speicherplatz der neuen Festplatte dem LVM zur Verfügung.

11.2.2.5 Vergrößern des Logical Volumens

Der zusätzliche Speicherplatz kann nun durch LVM-Befehle an die *Logical Volumens* vergeben werden. Im folgenden Beispiel vergeben wir den kompletten neuen (freien) Speicherplatz an das *Logical Volume „/hohe“*.

```
Beispiel:# lvresize --extents +100%FREE vg_ucs/homefs
```

root@server:~# lvresize --extents +100%FREE vg_ucs/homefs
Extending logical volume homefs to 180,01 GiB
Logical volume homefs successfully resized
root@server:~#

Abb. 248: Ausgabe des Kommandos lvresize

Nachdem das Volume vergrößert wurde, muss noch das Dateisystem ebenfalls angepasst werden:

Beispiel:

```
# resize2fs /dev/vg_ucs/homefs
```

root@server:~# resize2fs /dev/vg_ucs/homefs
resize2fs 1.41.12 (17-May-2010)
Das Dateisystem auf /dev/vg_ucs/homefs ist auf /home eingehängt; Online-Grössenveränderung nötig
old desc_blocks = 7, new_desc_blocks = 12
Führe eine Online-Grössenänderung von /dev/vg_ucs/homefs auf 47188992 (4k) Blöcke durch.
_

Abb. 249: Ausgabe des Kommandos resize2fs

Dieser Vorgang kann einige Zeit in Anspruch nehmen. Damit ist die Vergrößerung abgeschlossen.

Alternativ könne auch nur ein Teil des neuen Speicherplatzes (z.B. nur 20GB) an das *Logical Volume* vergeben werden, der Befehl dazu würde dann lauten

Beispiel:

```
# lvresize --size +20G vg_ucs/homefs
```

11.2.2.6 Übersicht über die Logical Volumes

Die LVM-Konfiguration im Auslieferungszustand:

virtuelle Maschine	Volume Group	Logical Volume und Größe	Einhägepunkt und Verwendung
Server	„vg_ucs“	homefs (180 GB)	/home : Benutzerdaten
		rootfs (20 GB)	/ Root-Verzeichnis
		varfs (55 GB)	/var
opsi-Server	vg_ucs	rootfs (20 GB)	/home
		varfs (100 GB)	/var

Tabelle 7: LVM-Konfiguration der paedML Linux

Landesmedienzentrum Baden-Württemberg (LMZ)
Support Netz
Rotenbergstraße 111

70190 Stuttgart

© Landesmedienzentrum Baden-Württemberg, 2015